Investigating users' readiness to trade-off biometric fingerprint data

Anonymous ISBA 2015 submission

Abstract

Biometric-based authentication is a growing trend. While this trend is enabled by the introduction of supporting technology, the use of biometrics introduces new privacy and ethical concerns about the direction of authentication. This paper explores willingness of users to share biometric information and therefore take advantage of these technological advances. Specifically, this study examines, by means of an experiment, the readiness of users to provide their fingerprints and the factors that affect this decision. In addition the study surveyed 100 participants, and found that most users are currently not willing to share their fingerprints with an e-commerce site for any feasible reward.

It was found that while the financial incentive was a factor in the participants' decisions, perception of risk influenced by being exposed to previous cyber-attacks as well as the participants' self-efficacy had significant effect on the participants' decision making. The study also examined how comfortable participants are to share different types personal information with different entities, and found that participants make context-based decision about sharing their personal data.

The results of the study indicate that many users have concerns sharing their fingerprints with commercial companies. As new systems are being deployed, a better understanding is needed about user perceptions and the factors that may cause reluctance to share fingerprint data, so they can be better addressed by system designers in the future.

1. Introduction

Biometric fingerprint data is currently used successfully for security purposes, such as crossing national borders [2] and in enterprises for employee authentication [14]. It offers the benefit of unique identification, which is imperative to these applications. In these cases, it is mandatory for the users to provide their personal data. However, utilizing biometrics for commercial purposes is a new trend that emerged due to the release of affordable fingerprint readers. This raises the question: *Will users be willing to provide this data voluntarily, as a trade-off for perceived incentives?*

Since biometrics can not be forgotten or lost, using biometrics for user authentication offers some benefits relative to passwords. However, the use of biometrics for authentication raises some well known issues. Gathering biometric information raises risks of it being misused. For example, it raises privacy concerns, and may lead to unintended consequences. Privacy allows the user to control access to his personal information and remain autonomous. Since biometrics cannot be changed, users may not have control over the system once the data is gathered, and they can not delete the data or limit the way it is being used. This limits the user ability to manage the future uses of their personal information and may cause them to be susceptible to privacy attacks.

Biometric information data storage may also be vulnerable to attacks, thus leading to data being stolen, compromised or lost [1]. This is a significant drawback, since unlike passwords, biometric data can not be revoked in case they are compromised.

In addition, since biometric information is not secret, it may be possible to gather without the person's consent. For example, pictures can be taken of a person's face, and users leave their fingerprints on devices they use. This raises the risk of a user being unknowingly tracked by certain systems [13]. It has also been shown that it is possible for attackers to create a duplicate of a fingerprint [18], which may render users susceptible to impersonation attacks.

Finally, relying on biometric information for user authentication raises additional ethical concerns. Traditionally, human recognition is an action with prior consent of the individual. Automatic recognition of humans, especially when relying on biometrics, may be unacceptable to users. For example, using biometric information instead of password limits the ability of the users to stay anonymous. Certain biometric information, such as fingerprints, can be used to identify a user against his will, when he could use an alias as his user name otherwise. Moreover, some biometrics, such as fingerprints and DNA, are used in criminal investigations and may therefore carry negative associations. Other concerns may be religious or cultural, as users may reject the use of biometrics based on historical associations, where Nazi Germany marked Jews with a tattoo. In addition, some people voice religious objections, as noted by a recent lawsuit [3].

Utilizing biometrics for commercial purposes relies on customers readiness to share such data. While there has been a wide body of research into mathematical methods of ensuring fingerprint privacy [26, 31], very little research has been conducted into users' readiness to share this data with commercial devices and applications, as well as other entities.

Contribution of this study This work takes an empirical approach to studying the factors that affect participants' readiness to share their fingerprints. It attempts to look at the question: *Are users willing to share their biometric data with commercial companies? What factors and trade-offs affect the user willingness to share their data?* The factors that were studied were trust, monetary rewards, previous exposure to cyber-attacks, demographic and professional parameters.

This study found that most users (60%) were not willing to share their fingerprints in exchange for a financial reward. The study found that while the financial incentive was a factor in the participants' decisions, perception of risk influenced by being exposed to previous cyber-attacks as well as the participants' self-efficacy had significant effect on the participants' decision making. It also found that the willingness to share this data was rising proportionally to the amount of the reward, with an average value of $44.10 reimbursement found for the study participants. Trust was found not to be a contribution factor to the users' decision making, as the same number of users were willing to provide their fingerprints to either a known or an unknown website. The participants were also surveyed about their willingness to share various types of data with different entities, finding that participants differentiate the willingness to share different types of data based on the application context.

2. Background and Related Work

Recent studies have looked into participants' willingness to accept using biometrics for different purposes. In a global survey conducted by Unisys, [5], US participants were asked where would providing biometric information would be acceptable, with 60% of the participants agreeing it is acceptable to provide it at airport security checkpoint, but only 21% believing it is acceptable to provide it on social media sites. In another survey conducted in Germany, half of the German participants voiced privacy concerns when asked about using electronic facial recognition to identify known criminals.

Security and privacy concerns about using biometrics were also discussed by Prabhakar et. al. [25], who pointed out that lack of legislation to ensure proper use of biometrics and self-regulation may open the door to possible abuse of biometric information. A study by Pons et. al. [24] showed that participants are neither familiar, interested or experienced with using biometrics. Privacy and ethical concerns were also voiced by Jamieson. et. al. [19], who pointed our that even technology that uses algorithms to store fingerprints as statistical form may be misused or compromised in the future to recreate accurate depiction of the print.

Acquisti [6, 7] makes the argument that privacy is an economic problem, and that privacy is about trade-off: both individuals as well as organizations base their decisions regarding revealing certain private information on the perceived benefits and costs associated with it. He further makes the argument that experimental economics can help understand how people make decisions about their personal information. This understanding can then help create improved policy and technology design changes.

Heckle et. al. [17] investigated the acceptance of biometric security services and showed that participants felt more comfortable using their fingerprints biometric to secure personal purchases than when asked to secure corporate purchases. That study, similar to the one presented in this paper, points to the fact that users are willing to ignore the risks in sharing fingerprint biometrics to gain perceived personal benefits.

2.1. Emerging Technology

This section provides an overview of some of the devices and applications that have recently introduced fingerprint-based authentication.

iPhone 5S Touch ID The iPhone 5S device allows users to scan their fingerprints and use it for authentication. The Touch ID primary feature allows a phone owner to use the touch ID instead of a pass-code to unlock the phone. The user first initializes the phone by providing his fingerprints. Afterwards, the user unlocks the phone by touching the home button once and then lightly keeping the finger on the home button. In addition to unlocking the phone, the user can also use the Touch ID to purchase items at the ITunes store, App store and iBooks store.

Touch ID does not store the images of the user fingerprints, but a mathematical representation of those fingerprints. Therefore, Apple says it is not possible to reverse engineer any of those fingerprints. In addition, the fingerprint data is encrypted and the data is being used only by a security application called Secure Enclave. The data can not be accessed by any other applications or the IOS and is not being uploaded to any servers of the iCloud.

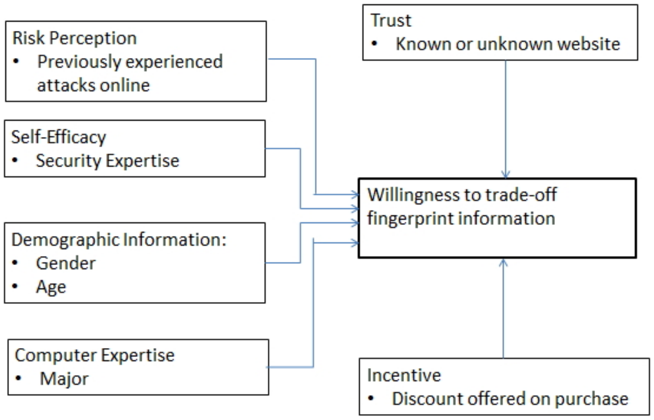
Laptops with fingerprint reader: Multiple laptops integrated in the last few years a fingerprint reader. One of them is the HP SimplePass Fingerprint reader, which integrates the fingerprint reader into HP laptops. The device allows enrolling the user fingerprints into the device. The user can then use these fingerprints to register or manage their logons for applications and websites. The device does not specify how the fingerprint data is protected from attackers. Similarly, USB devices that connect to laptops, including the Microsoft Fingerprint Reader, have been developed and released.

Applications accepting fingerprint authentication: Paypal has recently announced the availability of the PayPal app with fingerprint authentication on the new Samsung Galaxy S5 as well as other Samsung devices [12]. Users can login with their fingerprint to shop at millions of merchants that accept PayPal on mobile web sites, mobile apps and in stores. This demonstrates the growing trend in capturing and using fingerprints, who rely on the user willingness to share it and its mental belief that using fingerprints offer a security benefit.

3. Study Hypotheses and Approach

This work explores the hypotheses that the willingness to share biometric information with a commercial website is affected by a few variables, relating to the participants knowledge, risk perception, self-efficacy, trust and demographic information, as appears in Figure 1. The assumption is that while people will be more willing to trade their fingerprints for a certain incentive, other variables may cause certain biases that will prevent certain users from engaging in such data sharing.

Figure 1. Research model and hypotheses


Risk Perception
• Previously experienced attacks online
Self-Efficacy
• Security Expertise
Demographic Information:
• Gender
• Age
Computer Expertise
• Major
Trust
• Known or unknown website
Willingness to trade-off fingerprint information
Incentive
• Discount offered on purchase

Following are the hypothesis tested in the study:

H1: Risk Perception will affect willingness to share biometrics. Familiarity with risks may lead individuals to view the cost of sharing as high relative to the reward, since familiarity with risks has been shown to skew the individual's perception of their likelihood [20]. Participants who experienced a previous attack may become risk averse and want to limit the possibility of a loss (and the experience of emotional pain due to such loss). Therefore, the hypothesis is that a higher risk perception with respect to online activity will lead to a lower willingness to share biometric information,

H2: Self-Efficacy affects willingness to share. Self-efficacy has been correlated to behavior and attitude. Specifically, self-efficacy is a direct predictor of intention and behavior, as it pertain to a person's feeling of control over his behavior and environment [28]. The hypothesis tested in this study is that participants with higher self-efficacy will be more likely to share their data, as they feel more in control of their decisions and can make more rational choices regarding the benefits of sharing their fingerprints. Self-Efficacy is measured by asking the participants about their security expertise.

H3: Computer knowledge affects willingness to share. As more and more security classes are offered to computer science students, it is assumed that participants from CS background will be more security-oriented and be less willing to share their data. The hypothesis tested in this study is therefore that participants with higher experience working with computers will be less likely to share their data.

H4: Gender and age will affect willingness to share biometrics. Surveys show that older adults are less likely to use new technology [27]. The assumption in this study is that younger people will be more willing to accept new technology and new programs and will be more willing to share their fingerprints. Also, gender may play a role in the willingness to share fingerprints. While women have been shown in general to be less risk taking [9, 16], they have been shown to be more likely to embrace new technology[10]. Therefore, the hypothesis is that age will be inversely related to the willingness to share fingerprints, and that women are more likely to accept fingerprint readers.

H5: Trust will affect willingness to share. Trust is a major component affecting decision making. Participants are more likely to enter transactions with trusted authorities. Trust has been shown to directly affect users' decision to engage in electronic commerce [21]. The hypothesis tested in this study is that participants will be more likely to share their information with a trusted website.

H6: Incentive will affect willingness to share. Individuals are willing to trade-off privacy for certain benefits (Acquisti [6]). Therefore, offering an incentive to participants will raise the likelihood of them sharing their biometric information, vs. considering this without any incentive. The hypothesis of this study is that participants will be more likely to share their fingerprint if a higher incentive is offered. This is tested by examining the increase in the number of participants who are willing to trade their fingerprints for a rising incentive.

H7: Intention and attitude towards sharing biometric data affects willing to share. Ajzen [8] et. al. claimed that intention is the most important cause of people's behavior. In this study, we look at the participants' predicted behavior, as measured in a role-play experiment, vs. their attitude, when asked if they will share their biometric information with a website (without considering any compensation). The hypothesis is that intention will be highly correlated to the willingness to share biometric data.

H8: Willingness to share of data is based on context. Context is a major factor in the design of many new devices [29], and Nissenbaum [23] has argued that people are not as concerned with sharing their information in general, but are concerned about it being shared in inappropriate contexts. Two specific cases are examined to evaluate this hypothesis. The first is that people differentiate between revocable and non-revocable data, and may be more willing to share types of data that can be revoked than share fingerprint data. The second is that participants will be more likely to share their personal and biometric data with authority than with other entities.

4. Experimental Setup

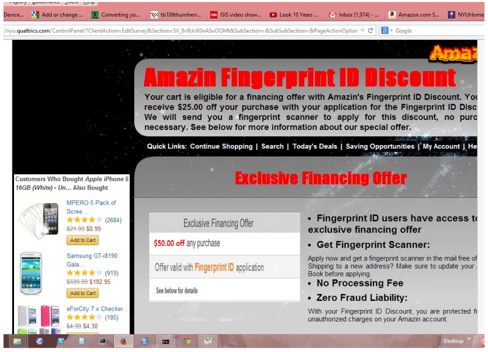
To examine the issues listed in the previous section, an experiment and an online survey questionnaire were prepared (survey appears online [4]). The study was conducted in a northeastern university. A total of 109 people originally started the study, with 9 deciding to quit at the beginning or in the middle so their results were not used, leaving a total of 100 participants who participated in the experiment and filled the survey. These included 24 women and 76 men. The participants were volunteers and no compensation was provided. 73% of the participants were under 24 years old, 22% were between 25 and 34 years old, and the rest (5%) were over 44 years old.

The experiment included two mock website snapshots that were shown to the users. Half of the users were shown one website (which duplicated the well known and familiar 'Amazon' website). The other half of the users were shown a new website which was designed by the authors, called 'Amazin' (see Figure 2. The users were asked to look at them and respond as if they were indeed shopping on the website for a tablet computer. In particular, they were asked if they would be willing to share their fingerprints for a discount of $50 when shopping on that website. The participants were asked to sit next to a computer which had a mock fingerprint reader attached to it.

It should be noted that the experiment was similar to real-life offers that frequently are shown to buyers by the Amazon site, which offer a discount of either $20 or $50 if the users open an Amazon credit card account. Therefore, this is a feasible scenario that companies may use to get buyers to enroll in a new program. The acceptance of such an offer and the amount indicates the trade-offs users are willing to make in return for the offered reward, and offer a method to evaluate the value of the information provided in financial terms.

Afterwards, the experiment users were asked to respond to the rest of the questions in the survey. The survey included 13 questions and took about 15 minutes to complete. Only adults were surveyed (18 years or older).

Figure 2. A web-page created for the survey, presenting a discount to the users if they enrolled in a fingerprint program.



Amazin Fingerprint ID Discount

Your cart is eligible for a financing offer with Amazin's Fingerprint ID Discount. You receive $25.00 off your purchase with your application for the Fingerprint ID Disc We will send you a fingerprint scanner to apply for this discount, no purc necessary. See below for more information about our special offer.

Quick Links: Continue Shopping | Search | Today's Deals | Saving Opportunities | My Account | He

Customers Who Bought *Apple iPhone 5 16GB (White) - Un...* Also Bought

MPERO 5 Pack of Scree... ★★★★☆ (2684) ~~$21.99~~ $0.99 Add to Cart

Samsung GT-i8190 Gala... ★★★★☆ (919) ~~$599.99~~ $192.95 Add to Cart

eForCity 7 x Checker... ★★★★☆ (185) ~~$4.99~~ $4.30

Exclusive Financing Offer

Exclusive Financing Offer

$50.00 off any purchase

Offer valid with Fingerprint ID application

See below for details

- **Fingerprint ID users have access t exclusive financing offer**
- **Get Fingerprint Scanner:**

Apply now and get a fingerprint scanner in the mail free of Shipping to a new address? Make sure to update your Book before applying.

- **No Processing Fee**
- **Zero Fraud Liability:**

With your Fingerprint ID Discount, you are protected fr unauthorized charges on your Amazin account.

5. Results: Factors affecting willingness to trade fingerprint data

Following are the results obtained from the study:

H1: Risk Perception will affect willingness to share biometrics

The hypothesis is that a higher risk perception with respect to online activity will lead to a lower willingness to share the biometric information. The participants were asked about the activities they perform online and the vulnerabilities they experienced, including getting their account hacked, being victims of identity theft and having a malware or virus infect their computer.

The number of participants who encountered identity theft was very low (6), and 28% of the participants had their account hacked. However, the study found that the majority of the participants (61%) encountered a malware or virus on their computer.

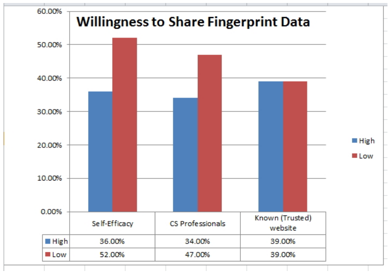
This hypothesis was supported, as people who experienced any cyber-attack were less likely to share their biometric information. Specifically, more than half of the participants (56%) who did not experience a virus attack would provide their fingerprints, but only 28% of people who were subjected to a virus attack would provide it. The difference was lower for people who had their system hacked, with 28% of people attacked willing to share their fingerprints vs. 43% of the participants who were not hacked expressing willingness to share this data. There were only six participants who experienced identity theft, of which a third would share their fingerprints. Overall, 30% of the people who were attacked would provide their fingerprints, while 56% of the people who were not attacked would provide their fingerprints $(Pearsoncorrelation = 0.243, p < 0.05)$.

Therefore, this variable was found to have significant correlation with the willingness to share fingerprints.

H2: Self-Efficacy affects willingness to share

Self-efficacy has been correlated to behavior and attitude. Specifically, self-efficacy is a direct predictor of intention and behavior, as it pertain to a person's feeling of control over his behavior and environment [28]. The hypothesis tested in this study is that participants with higher self-efficacy will be less likely to share their data, as they prefer to control the access to data. The results can be seen in Figure 3. The study found that 52% of the participants that had low self-efficacy were willing to share their fingerprints, vs. 36% of the participants who had high self-efficacy. This hypothesis was supported, as people with high security expertise were less likely to share their data ($Pearsoncorrelation = 0.215, p < 0.05$).

Figure 3. Willingness to share as a function of computer proficiency and security expertise. Participants with higher level of those traits were less likely to provide their fingerprints. On the other hand, the trust factor due to a known or unknown websites did not affect the users decision to share their fingerprints



.

H3: Computer knowledge affects willingness to share

The hypothesis tested in this study is that participants with higher experience working with computers will be less likely to share their data. The study found that participants who define themselves as computer professionals were less likely to provide their fingerprints. Overall, 34% of the participants that studied or worked in a computer-related field would provide their fingerprints, vs. 47% of the participants who were not from a related field. However, this hypothesis was not found to be statistically significant ($C = 0.121, p < 0.25$), therefore it is not supported and more data is needed to prove or disprove it.

H4: Gender and age will affect willingness to share biometrics

The hypotheses were that age will be inversely related to the willingness to share fingerprints, and that women are more likely to accept fingerprint readers. The study did not find differences based on age. However, it did found difference in willingness to participate based on gender, where 54% of women were willing to share their fingerprints compared to 34% of men. The hypothesis related to age was not supported, while the hypothesis related to gender was supported (C = 0.175, p ¡ 0.1) , with women more likely to be willing to share their fingerprint data.

H5: Trust will affect willingness to share

The hypothesis tested in this study is that participants will be more likely to share their information with a trusted website. Therefore, to test this, half of the participants were shown the a mock-off of a known (and widely trusted) website (Amazon) and half were shown an unknown website that was created for this study. The results show that there was no difference between the participants' readiness to contribute their fingerprints for either site, pointing to the fact that the participants initial tendency to contribute their fingerprints overcomes the effect of encountering a trusted website.

Further, when comparing between the average monetary values that the participants were willing to trade-off for on the 'known' Amazon website vs. the 'unknown' 'Amazin' website, the values were found to be very close. The'Amazin' participants indicated an average compensation equal to $42.56 would be needed while the 'Amazon' participants chose an average value of $45.78.

Therefore, this hypothesis that trust will affect willingness to share was not supported by the result of the study.

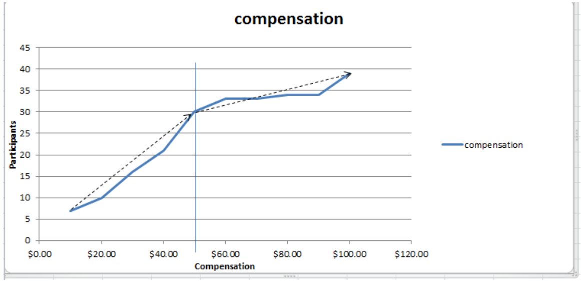
H6: Incentive will affect willingness to share

The hypothesis of this study is that participants will be more likely to share their fingerprint if a higher incentive is offered. To test this, the users were asked for what amount of money they would be willing to share their data. Originally, the participants were asked if they would trade-off the data for $50. People who were originally willing to share their data for this amount were asked what would be the minimum amount they would share the information for (5 values were provided between $10 and $50). People who were not willing to share their data for that amount were asked about higher amounts ($60, $70, $80, $90 and $100). The graph with the results can be found in Figure 4. It can be seen that the trend-line for people who are willing to share their information for less than $50 is steeper than the one for people who are willing to share it for more than that amount. This points to the fact that any additional compensation above a certain number will have lower affect on increasing the willingness of users to participate in such a program.

Another finding was that when asked about their willingness to share fingerprints with commercial sites such as Amazon, without considering any incentive, only 7% of the participants expressed they were comfortable with sharing this data. This demonstrates that while the original intention of most users may have not been to share their fingerprints, providing an incentive outweighed the original reluctance of many of the participants and caused them to accept the trade-off.

Calculating the average value of the fingerprints to the users who are willing to share their fingerprints provides a value of $44.10. This value is close to the original tested

Figure 4. Willingness to share as a function of compensation. Two different trend-lines can be viewed, where the people who are willing to share their information for $50 or less is more steep than the one for people who are willing to share their information for more than that



value ($50), indicating that framing of the initial value did have a large affect on the user response. Overall, 30 people responded to the original questions positively, indicating that they would provide their fingerprints for $50. Only 9 people said they would not provide their information for that amount but would provide it for a higher discount. This also supports the notion that people who are willing to share their information would do that for less than the originally specified value.

Overall, the study found that higher incentive raised the participants willingness to share this information ($PearsonCorrelation = 0.948, p < 0.001$). Therefore, this hypothesis was supported.

H7: Intention and attitude towards sharing biometric data affects willingness to share

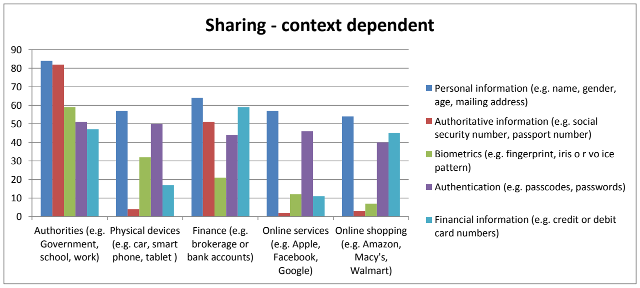
The hypothesis is that intention will be highly correlated to the willing to share biometric data. This study found that while 7% participants felt comfortable providing their biometric data for online services, 39% were willing to provide it when considering an incentive. All of the participants that said they were comfortable providing their fingerprints were also willing to share it for an incentive. However, 32%, who said they were not comfortable sharing their fingerprints (when no incentive was considered) were willing to trade-it when offered an incentive. Therefore, the study found that positive intention does affect willingness to share, but negative intention can be overcome with incentive. Overall, a significant correlation was found between the intention and the actual willingness to share ($C = 0.343, p < 0.001$). Therefore, this hypothesis was supported.

H7: Willingness to share data is based on context

The hypothesis is that people may be more willing to share other types of data that can be revoked than fingerprint data. Also, participants will be more likely to share this data in different contexts, such as with more authoritative entities.

Examination of the results (Figure 5) shows that participants were more willing to share different types of data with authorities than with other entities. Finance came in a second place, with more than 40% of the participants willing to share most kind of data with financial websites than other commercial sites. However, biometrics was indicated to be less accepted than other kind of data when considering sharing with financial institutions. Participants felt more justified in sharing fingerprint data with authorities and physical devices, followed by financial institutions, online services (Facebook, Apple, etc.) and least of all online shopping sites (such as Amazon). Similar values were received from passwords for all the contexts, while more participants stated they would feel comfortable sharing credit card information with authorities, financial institutions and online shopping sites than physical devices and online services. This shows that the decisions to share the different data type was based on the context and supports the idea that people object to inappropriate, improper sharing of information [23].

Figure 5. Participants indicated their willingness to share different biometric or personal data with different types of sites. The study indicated that the context of the website was a key to the participant's willingness to share this information, indicating users favor context-based authentication.



When examining the likelihood of participants to share revocable data (passcodes, passwords, credit card and debit card information) vs. the other types data, which are harder to revoke (such as name, gender, social security and biometric information), no significant difference was found, with 39% of the participants feel comfortable sharing a non-revocable data type vs. 36% comfortable sharing revocable data. This was detected with a statistically significant correlation, indicating a consistent trend for all of the participants ($paired-samplest-testcorrelation = 0.569, p < 0.001$). Therefore, this hypothesis was not supported.

However, the results did show that participants are more likely to share their data with authoritative entities, with participants likely to share their data 63% of the time with authorities vs. 32% with non-authoritative entities. A statistically significant correlation was detected between the amount information the participants are willing to share with authorities and non-authorities, indicating a consistent trend ($paired-samplest-testcorrelation = 0.427, p < 0.001$) . Therefore, this hypothesis is supported.

5.1. Study Limitations

Following are several limitations that may affect the results and therefore more work may be needed in order to generalize them to the entire population. The study was conducted in a Northeastern University, and therefore many of the participants were students or university employees. In addition, while the work includes a ‘role-play’ experiment, which is a widely accepted research method ([22, 30]), user behavior may be different in real-life situations, when financial or other types of incentives are offered. Future studies are therefore desired to better understand the response in a real-world scenario among the general population.

6. Conclusions and Future Work

This study examined different variables that may affect the participants’ willingness to share biometric data. Some of the studied variables support rational decision making, such as incentives and self-efficacy, whereas other variables may be based on biases, such as higher risk perception and fear of loss due to previous exposure to cyber-certain attacks. The study shows that currently such biases outweigh financial incentives for many of the participants.

This study includes the first experiment that the authors are aware of that examines the willingness of users to share their fingerprint data for certain financial rewards. The study shows that most of the participants are not willing to share their fingerprint data in commercial setting. This finding raises the need for additional investigation, as new commercial systems that offer fingerprint authentication come out. It also showed that monetary reward does affect the users’ willingness to share, with an average reward value of $44.10 indicated as an acceptable monetary trade-off discount for this data.

The study also showed that many participants who stated they do not feel comfortable sharing their data with commercial entities (such as Amazon), were willing to share it when offered financial incentive. Therefore, this points to the fact that the cost perceived with sharing the fingerprints for these participants (32% of the participants) is less than the benefit of receiving a monetary compensation. While this study only looked at financial compensation, this suggests that other perceived benefits that commercial entities may offer, can raise the probability of participants sharing this data.

From the parameters examined, this work found that previous familiarity with cyber-attacks has the most significant correlation to willingness to provide fingerprint information, suggesting that people make a connection between potential vulnerability associated with sharing their fingerprint data to other cyber-attacks. This shows a bias within victims of previous attacks, as all users may be vulnerable to such attacks, but users who have been exposed to them are more reluctant to provide their fingerprints voluntarily for commercial purposes.

Participants with higher self-efficacy were found to be less willing to provide their fingerprints. This suggests that providing fingerprints is deemed to be more risky by people who believe they have higher security expertise. In addition, women were found to be more willing to provide their fingerprints. This may suggests a lower perception of risk related to online activities, which is inline with the findings in a previous study, in which women were found to be more likely to respond more phishing emails [15].

When examining participants comfort with sharing different types of data, when no incentive is considered, the study found people felt more comfortable providing biometrics as well as other personal information to authorities than to other entities. Participants did not discern between revocable data (such as credit cards and passwords) and non-revocable data (such as biometrics, name, gender, etc.) and did not show preference towards disclosing revocable data for authentication.

The study participants did not base their decision whether to share biometric information on trust and familiarity with the website. This causes some concern, as the internet is an open medium, and anybody can start a website. If users do not take into account site familiarity, attackers can create new websites to get sensitive information from users. Examples of frauds that resulted from such websites are documented in the 2013 FBI Internet Crime Report [11].

Biometric fingerprint data is currently used successfully for security purposes, such as crossing national borders [2] and in enterprises for employee authentication [14]. However, utilizing biometrics for commercial purposes is a new trend, that emerged due to the recent release of affordable fingerprint readers, and relies on the willingness of the user to share this data voluntarily. This study examines that factors that affect the users’ reading to share this information in e-commerce, and shows that both rational as well as biased factors affect the participant’s decision. The study points out to the possibility that incentives may cause certain participants to provide biometric data regardless of the trust and reputation of the entity. It also shows that many users may be reluctant to use fingerprint authentication on commercial websites. This raises the need for additional investigation, as new commercial systems that offer fingerprint authentication come out.

7. Acknowledgments

This work was supported in part by the NSF (under grant 1228842). The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of any of the sponsors.

References

[1] Biometrics: An Overview of the Technology, Challenges and Control Considerations. http://bit.ly/1ugcaBA, 2004.

[2] US Visit - Entry/Exit system. http://www.immihelp.com/visas/usvisit.html, 2004.

[3] 2013 Internet Crime Report. http://bit.ly/1uSNAK2, 2013.

[4] Fingerprint data survey. http://bit.ly/1woXqon, 2014.

[5] Unisys Security Index: GLOBAL SUMMARY. bit.ly/Zs5K9D, 2014.

[6] A. Acquisti. Privacy & Behavioral Economics: The Paradox of Control & Other Studies. http://www.heinz.cmu.edu/ acquisti/papers/acquisti_privacy_behavioral_economics.pdf, 2010.

[7] A. Acquisti. The Economics of Privacy: Theoretical and Empirical Aspects. http://cusp.nyu.edu/wp-content/uploads/2013/09/C03-acquisti-chapter.pdf, 2013.

[8] I. Ajzen. *From Intentions to Actions: A Theory of Planned Behavior*. 1985.

[9] J. Byrnes, D. Miller, and W. Schafer. Gender differences in risk taking: A meta-analysis. *Psychological Bulletin*, 125(3):367–383, 1999.

[10] D. S. Consulting. Women more likely to use connected living technology than men. http://bit.ly/1AOtWQO, 2014.

[11] FBI. 2013 Internet Crime Report. http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf, 2013.

[12] FinExtra. PayPal adds fingerprint authentication to more Samsung devices. http://www.finextra.com/news/announcement.aspx?pressreleaseid=56577&topic=retail, 2014.

[13] E. F. Foundation. Biometrics: Who's Watching You? . https://www.eff.org/wp/biometrics-whos-watching-you, 2003.

[14] W. Fumy and J. Sauerbrey. *Enterprise Security: IT Security Solutions – Concepts, Practical Experiences, Technologies*. Siemens, 2006.

[15] T. Halevi, J. Lewis, and N. Memon. A pilot study of cyber security and privacy related behavior and personality traits. *PSOSM 13*, pages 737–744, 2013.

[16] C. R. Harris and M. Jenkins. Gender Differences in Risk Assessment: Why do Women Take Fewer Risks than Men? *Judgment and Decision Making*, 1(1):48–63, 2006.

[17] R. R. Heckle, A. S. Patrick, and A. Ozok. Perception and acceptance of fingerprint biometric technology. *SOUPS '07*, pages 153–154, 2007.

[18] A. M. Holland-Minkley. Biometric Devices and Fingerprint Spoofing. www2.washjeff.edu/users/ahollandminkley/biometric/, 2006.

[19] R. Jamieson, G. Stephens, and S. Kumar. Fingerprint Identification: An Aid to the Authentication Process . *INFORMATION SYSTEMS CONTROL JOURNAL*, 1, 2005.

[20] D. Kahneman. *Thinking, Fast and Slow*. Farrar, Straus and Giroux, 2011.

[21] D. J. Kim, D. L. Ferrin, and H. R. Rao. A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decis. Support Syst.*, 44(2):544–564, Jan. 2008.

[22] N. Malhotra, J. Hall, M. Shaw, and P. Oppenheim. *Essentials of Marketing Research, An Applied Orientatio*. Pearson Higher Education AU, 2007.

[23] H. Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, Stanford, CA, USA, 2009.

[24] A. P. Pons and P. Polak. Understanding user perspectives on biometric technology. *Commun. ACM*, 51(9):115–118, Sept. 2008.

[25] S. Prabhakar, S. Pankanti, and A. Jain. Biometric recognition: security and privacy concerns. *Security Privacy, IEEE*, 1(2):33–42, Mar 2003.

[26] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle. Generating cancelable fingerprint templates. pages 561–572, 2007.

[27] P. Research. Older Adults and Technology Use. http://www.pewinternet.org/2014/04/03/older-adults-and-technology-use/, 2014.

[28] R. Schwartzer. Self-efficacy. http://1.usa.gov/1swCbkZ.

[29] N. T. I. series. Location, Context, and Mobile Services. http://nokia.ly/1G5VSCL, 2009.

[30] H. Stanton, K. W. Beck, and E. Litwak. Fingerprint Identification: An Aid to the Authentication Process . *American Journal of Sociology*, 62(2), 1956.

[31] Y. Sutcu, Q. Li, and N. D. Memon. Secure Sketches for Protecting Biometric Templates. Security and Privacy in Biometrics. *Security and Privacy in Biometrics*, pages 69–104, 2013.