Legal And Ethical Responsibilities In Mobile Payment Privacy

John Selvadurai

Abstract: Mobile payment is the new trend in the payment technology sector. The ecosystem of mobile payment is complicated and consists of multiple dimensions. Securing consumer privacy is an important aspect in any type of payment industry. Since the mobile payment industry is in its infancy, the requirements for respecting privacy are not too clear. This paper discusses the legal and ethical responsibilities of the individuals and organizations in the mobile payment industry to protect consumer privacy. As part of the discussion, firstly, the main types of mobile payment methods are explained. Secondly, the legal requirements of the privacy protection are analyzed. The main privacy aspects of Gramm-Leach-Bliley Act are explored in order to examine the legal requirements. Thirdly, the privacy concerns in the mobile payment methods are discussed as they relate to Gramm-Leach-Bliley Act. Finally, this paper recommends several guidelines to improve and protect consumer privacy in the mobile payment industry. This paper concludes with the ethical requirements of the businesses to build the trust from the consumers by protecting their privacy.

Index Terms: Carrier based billing, GLBA, Image scanning, Mobile Payment, NFC, P2P Payment, Privacy.

1 Introduction

Mobile Payment is a fast growing technology in mobile application development. There are many different types of payment applications for mobile devices available in all major mobile platforms. The ecosystem of mobile payment consists of many parties. Traditional payment systems typically involve the consumer, the receiver and the financial institution that facilitates the transaction. Usually the financial institution is a bank that provides services to the consumer. In the mobile payment life cycle, in addition to the traditional players, there will be the mobile application provider, third party application service providers and intermediate payment facilitators. Since there are many layers involved in mobile payment, controlling their own personal data is a challenge for the consumers. Because of the fast paced mobile application trend, there is little time and effort spent on protecting consumer data by the businesses that are developing mobile payment applications. This fact also introduces a challenge in the adoptability of mobile payments because consumers are waiting until secure standards are enforced. This paper underscores the legal and ethical need for technology builders to consider privacy in mobile payment.

2 Main categories of Mobile Payments

There are numerous mobile payment applications available for consumers. Currently available mobile payment applications can be categorized in five major types:

1. NFC Mobile Payment
2. Cloud Based Mobile Payment
3. Image Based Mobile Payment
4. Carrier Based Mobile Payment
5. Proximity Based Mobile Payment
6. Mobile P2P Payment

- *John Selvadurai is currently pursuing Doctoral degree program in Technology Management in Indiana State University, Terre Haute, Indiana, USA,PH-530 680 8184-mail: sjohnandrew@gmail.com*

2.1 NFC Mobile Payment

Near Field Communication (NFC) is a contactless communication technology standard that allows devices to exchange data through radio communication [1]. In order to perform such exchange both devices must be placed in close proximity. An NFC enabled phone is embedded with a special chip that can hold account information. Typically, when the mobile device is held closer to the reading device the payment information is transferred to the reading device [2]. This functionality is very similar to how contactless payment cards work. Therefore the security of the payment is similar to the security of contactless payment cards. The main advantage of NFC payment is that the information can be read by the reader even if the phone is powerless. Since it is common that phones loose charge in long distance traveling, other payment applications are no use. The main restricting challenge is the limited number of NFC enabled handsets and readers available worldwide. Since the main benefit of using mobile payment methods is to avoid carrying wallets, the users still have to carry wallets along with NFC payment devices if NFC readers are not available in every location. Also, the physical procedure of tabbing or waving the smartphone to the reader is almost same as swiping a credit card on credit card reader. This challenges the vendors/retailers to change already functioning credit card infrastructure to a NFC based framework.

2.2 Cloud Based Mobile Payment

He bank. Unlike NFC payment method, payment account information is stored remotely in the cloud system and not saved in the mobile device. This type of data storage provides greater ability to secure the privacy data in the cloud using traditional methods.

2.3 Image Based Mobile Payment

In image based mobile payments, an image is used to hold necessary information. An image can be a standard bar code, 2D bar code such as QR code or a photo. Technically, these images contain the payment information and by scanning the image via the mobile device's camera, the payment information is transferred. The payment information in the images is encrypted to protect unauthorized information extraction [4]. Since images can be generated with a minimum level of effort, this payment method doesn't need any additional hardware to be installed. This can be considered the

advantage of image based payments over NFC payments in spreading worldwide.

2.4 Carrier Based Mobile Payment

This payment method takes place via mobile carriers. In carrier based mobile payment method, purchases are billed through the carriers. In other words, cellphone carriers play the role of a financial institution. When the user completes a purchase, the transaction is completed with two-factor authentication. The consumer enters the mobile number and receives a one-time password or pin to the mobile phone. Upon entering that pin or password for verification the authentication is confirmed [5]. The cellphone carrier acts as a financial organization and completes the transaction. The necessary amount will be claimed either from a prepaid account of the user or on the monthly cellphone bill.

2.5 Proximity Based Mobile Payment

Payment is initiated via geographical location services. When the consumer's mobile device enters the virtual perimeter of the merchant, the payment activity is initiated. The identity of the consumer will be verified by requesting pin or name. The payment information is exchanged via internet just like in cloud based payments [4]. Some proximity based apps allow the consumer not to even touch the smartphone when using this payment method. When the user enters the virtual zone of the merchant, user information is automatically logged into the merchant's device through geo location based services. Upon verifying the identity, either a name, pin or photo, the merchant will initiate the payment. This method carries higher potential of risks because there are no clear security measures established in the case of thefts of mobile phones.

2.6 Mobile P2P Payment

Mobile Person to Person payment method allows transferring funds from one individual's account to another by entering email, phone number or another type of identifier in the mobile application [6]. PayPal mobile app is a common example of such method. In general, this method is combined with other methods such as NFC and image based payment systems to provide a robust payment application.

3 Privacy Protection from Gramm-Leach-Bliley Act

Gramm-Leach-Bliley Act (GLBA) was enacted in 1999 to modernize the financial services industry. GLBA provides limited protections against selling personal financial data and prohibits the practice of obtaining personal information through false pretenses [7]. The primary purpose of GLBA was to end the regulation that prevented the merger of various financial service providers. Under GLBA, different financial services such as banks, insurance companies and stock brokerage can merge together to provide better services to the consumers. However, these type mergers also introduced the risk of exchanging privacy data between different entities without the consent from the consumer. Therefore, GLBA also addressed this concern by providing certain privacy protections to consumers. The following section reviews certain important aspects of GLBA regarding privacy.

3.1 Protection of Nonpublic personal information

In section 501 of GLBA, financial institutions are obligated to protect the security and confidentiality of their customer's nonpublic personal information [8]. Nonpublic personal information is defined as any information personally identifies the consumer and that information was provided by the consumer to a financial institution or obtained by the financial institution from a transaction or any other way. Also, section 501 compels financial institutions to ensure the safety of the consumer privacy data by establishing appropriate administrative, technical and physical safeguards. Therefore, financial institutions are required to protect personal information of consumers from any unauthorized access or anticipated threats.

3.2 Obligation to provide Notification

Under section 502 of GLBA, financial service providers are required to notify consumers about their information sharing practices. Financial institutions must do that once initially at the time when someone joins as a consumer and annually thereafter [8]. Basically, financial service provider should reveal how the nonpublic information of the consumer will be disclosed to affiliated and non-affiliated organizations. Also, the details of how nonpublic information is protected and what might happen to that information in the event of consumer termination. The format of the notices is encouraged to be clear and conspicuous. The consumer must also be informed of the right to opt-out from sharing personal information. A reasonable opportunity must be given to the consumer to opt-out in case the consumer chooses not to provide or share the nonpublic information. Often the practice of this obligation is not direct. Typical privacy notices often inform the consumers that their personal information will be shared but do not include information about what is shared and for what purpose.

3.3 Opt-out option

GLBA provides an opt-out option to the consumers if they do not wish to share their nonpublic personal information [8]. That means consumers can direct the financial institutions not to share their nonpublic information to third party nonaffiliated organizations. This provision gives privacy protection to the consumers by allowing them to choose what to do with their nonpublic information. Even though opt-out option gives some level of protection; still there are privacy concerns in this option. Even with the opt-out option, the consumer cannot stop any sharing of nonpublic personal information between affiliated organizations. An affiliated organization means any company that is controlling or controlled by the financial institution or commonly controlled by another company. However, an exception is allowed if the financial institution is giving nonpublic information to a nonaffiliated third party to perform services on their behalf [9]. For example, a nonaffiliated third party marketing agency that provides marketing services to the financial institution could receive consumer nonpublic information legally. Once these nonaffiliated third party services get the nonpublic account information, nothing restricts them from sharing the information with their affiliated entities. In this way, nonpublic information could spread across the industry even under GLBA's restriction. However, this exception is not applied in disclosing credit card numbers or bank account numbers to the marketing agency in order to provide services. Disclosing such

credit card and bank account numbers to nonaffiliated third parties is still prohibited. This opt-out option has a huge implication in practical procedures of financial organizations. Many financial organizations provide notification of the sharing of nonpublic information but it is the consumer's responsibility to inform them not to. By default, if the consumer doesn't respond in the required number of days that is considered as the consumer's acknowledgement that sharing nonpublic personal information is allowed. Often, consumers do not read the entire opt-out agreement and unknowingly acknowledge the sharing practice. This type of application of GLBA actually puts responsibility on the consumer's side rather than on the service provider to make the efforts not to share personal information.

3.4 Pretexting

GLBA makes pretexting illegal. Pretexting is the practice of collecting personal information under false pretenses by social engineering. An example of pretexting practice is posing as a member of an authority group such as law enforcement or potential employers and conducting legitimate processes like surveys of unsuspecting consumers. Through the questions of the survey, the individual who is posing as an authority figure will extract personal information from the consumer. Such practices are prohibited under GLBA.

5 Privacy Concerns in Mobile Payment Systems

Many mobile payment developers consider themselves belonging to technology industry and not to the financial industry. In reality, because mobile payments applications are facilitating payments, they are in fact providing financial services to the consumer. Therefore, they are subject to GLBA and other legal requirements in respecting consumer privacy.

The main aspect to be considered in consumer privacy is the protection of nonpublic information of the consumer. Mobile Payment Applications are dealing with greater level of nonpublic personal information such as consumer address, credit card accounts, and phone numbers. Often the secure data storage is overlooked in the development process and the mobile payment system is implemented with potential flaws in security. Because mobile payment systems are in the early stages not all the potential security lapses are explored yet. However, just like any other technology system, as time goes on and more consumers adopt the mobile payment methods, those security risks will be exposed. Next, the obligation to provide privacy notification is largely ignored by many current mobile payment applications. When the privacy notifications are given, most of the time, the information is not clear and hard to understand for common consumers. Often in privacy notifications, the message is not clear enough to determine what type of information will be gathered or shared. In a typical situation, the consumer agrees to privacy notification without understanding all the details because the terms are not clearly understood. In a similar pattern, the consumer doesn't choose the opt-out option because the option is not obvious from the notice. Especially in mobile payments when many intermediate parties are involved, consumers need to know their nonpublic information is protected and shared. Pretexting is a grey area in identifying the party involved in gathering personal information by posing as a legitimate purpose. Commonly, the consumer sees the mobile payment application as the only party involved in the payment process. However, there are many intermediate players in the mobile application facilitating payments and providing third party services. When these intermediate players gather nonpublic information about the consumer, it is unclear whether such practice will fall into pretexting or not.

5 Recommendations

The paradigm of mobile payment applications is complicated and does not have standardized regulations for all the possible risks. This paper recommends guidelines to mobile app developers and organizations to consider. These recommendations can be used to mitigate potential privacy risks and build consumer trust. The first recommendation is about the secure data storage of privacy information. It is encouraged not to store any nonpublic information in the mobile device. A mobile device should be used to read payment information but not to store nonpublic information. Various mobile payment methods handle nonpublic information differently. Cloud based systems typically handle the payment via their relevant cloud systems. On the other hand, NFC based mobile payment systems keep payment account details including nonpublic information in the NFC chip of the mobile device. Since NFC payment methods act similar to contactless payment card systems, the process of maintaining security and confidentiality is similar to contactless payment cards. Therefore storing payment information in the NFC chip is justified in that case. However, mobile application developers need to make sure appropriate measures are taken in such situations in order to prevent risks. Next recommendation is to use integrity and ethical sense in designing and implementing mobile payment applications. Because regulations and standards in the mobile payment industry are newer, it is possible that not all the security and privacy aspects are regulated. In this situation, mobile application builders should refrain from implementing unethical mobile payment processes by taking advantage of the lapses in the present legal system of mobile payment. Mobile payment applications are relatively different from traditional credit/debit card transactions. In traditional credit/debit card transactions, no party has access to all the pieces of consumer personal information. Information is typically split among various parties involved in the transaction. For an example, the vendor who receives payment from a credit card purchase will only know the purchase information and not necessarily any nonpublic information about the consumer such as full bank account number or address. On the other hand, the financial institution that offered the credit card would know the consumer contact information and the location of purchase but not necessarily the entire details of the purchased items. This balance in the payment echo system is challenged by mobile payment systems. Mobile payment applications have the ability to gather all the pieces of consumer nonpublic information and purchasing trends as well [10]. Mobile payment apps usually get consumer contact information by requiring consumers to register with them. Also, these mobile apps get bank or credit card information from the payment account details. In addition to all of them, mobile applications can also track the consumer's buying history and this type of data can be used to generate buying trends. All of the above can be constructed with little effort to satisfy privacy requirements. This type of data collection introduces huge concerns for privacy protection. There are many social media networks use such information collection to generate marketing data and eventually selling them to third party

advertisement organizations. Even though this practice is somewhat accepted in the technology industry, this paper advocates that mobile payment systems should not consider this practice. Since mobile payment systems fall into the financial service provider category, mobile application developers have the greater responsibility to protect such privacy data. The final recommendation is to implement a Do Not Track mechanism in the mobile application as it is encouraged by FTC [11]. DNT mechanisms will allow consumers to control tracking programs. Mobile application developers usually use third party controls in their applications to introduce already built-in features. From the technology perspective, such practices are encouraged in order to build systems in a faster way without rebuilding the entire system. In certain situations such third party applications provide new features such as tracking the location of the mobile application. However, some third party applications have tracking ability or advertisement services built in it. Therefore it is extremely important for mobile application developers to review and understand completely the functionalities and features of the third party controls prior to implementing them in their own mobile application.

6 Conclusion

Mobile Payment industry is complicated with many layers of players involved. Because of the nature of these multiple layers in a single transaction, consumer privacy data is spread through each layer. However, mobile application has the technical ability to collect the full details of consumer nonpublic information. If the consumer gives permission to the mobile payment application to collect their privacy data, it is not legally or ethically wrong to do so. But it is extremely important to protect such data from going to unintended parties. The business organizations who build mobile applications have the responsibility to protect consumer privacy data. It is the right thing to do legally and ethically. There are possibilities to work around the legal requirements and still be able to share consumer privacy data with third party organizations without the full consent of the consumers. But this paper advocates that mobile application organizations be always clear and concise about their intentions regarding the consumer and not to engage in any practice that is unintended by the consumer. It is the practice of building trust through transparency. Eventually, building trust with consumers is more critical for a successful business organization to thrive in the industry.

References

[1] Near Field Communication.org. “Near Field Communications: What is Near Field Communication?” [Online]. Available: http://www.nearfieldcommunication.org/ [May. 1, 2013]

[2] S. Yarbrough and S. Taylor. The Future of Payments: Is it in the Cloud or NFC?, [Online]. Available: http://www.tsys.com/Downloads/upload/Future-of-Payments-Cloud-of-NFC-WP-2.pdf

[3] D. Nicol, Mobile Strategy: How Your Company Can Win by Embracing Mobile Technologies. Upper Saddle River, NJ: IBM Press, 2013.

[4] Federal Deposit Insurance Corporation, “Mobile Payments: An Evolving Landscape”, Supervisory Insights, Winter 2012, January 2013. Available: http://www.fdic.gov/regulations/examinations/supervisory/insights/siwin12/mobile.html

[5] L. Bustos. (2012, September 4th). Carrier Billing: Understanding the Other Alternative Payment, [Online]. Available: http://www.getelastic.com/carrier-billing-understanding-the-other-alternative-payment/

[6] Smart Card Alliance. (September 2011). The Mobile Payments and NFC Landscape: A U.S. Perspective. [Online]. Available: http://www.smartcardalliance.org/resources/pdf/Mobile_Payments_White_Paper_091611.pdf

[7] Electronic Privacy Information Center. The Gramm-Leach-Bliley Act, [Online]. Available: http://epic.org/privacy/glba/

[8] Gramm-Leach-Bliley Act. Public Law 106-102-Nov. 12, 1999. Available: http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf

[9] R. Scott and A. Vanek, “Complying with the GLBA Privacy and Safeguards Rules”, Scott & Scott Compliance Simplified, Dallas, TX, [Online]. Available: http://www.scottandscottllp.com/main/uploadedFiles/resources/Articles/Article_Complying_GLBA.pdf

[10] Consumer Advertising Law Blog, (March 13, 2013), Mobile Payments: FTC Voices Concerns about Consumer Risks,[Online]. Available: http://www.consumeradvertisinglawblog.com/2013/03/mobile-payments-ftc-voices-concerns-about-consumer-risks-.html

[11] FTC Staff Report. (February 2013). Mobile Privacy Disclosures – Building Trust through Transparency. [Online]. Available: http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf