Cashless Society: Managing Privacy and Security in the Technological Age

Will Donohue
School of Integrated Sciences
James Madison University
Harrisonburg, VA, USA
donohuwe@dukes.jmu.edu

Zohaib Afridi
School of Integrated Sciences
James Madison University
Harrisonburg, VA, USA
alfridizx@dukes.jmu.edu

Kevin Sokolyuk
School of Integrated Sciences
James Madison University
Harrisonburg, VA, USA
sokolykp@dukes.jmu.edu

Tyler Bedwell
School of Integrated Sciences
James Madison University
Harrisonburg, VA, USA
bedweltd@dukes.jmu.edu

Emily R. York
School of Integrated Sciences
James Madison University
Harrisonburg, VA, USA
yorker@jmu.edu

Ahmad A. Salman
School of Integrated Sciences
James Madison University
Harrisonburg, VA, USA
salmanaa@jmu.edu

***Abstract*—A cashless society is an economic state which handles financial transactions not in the form of traditional mediums of currency, such as cash or coins, but by transferring digital data (usually by electronic means, such as credit cards and mobile data) between participating parties.**

Participants of a cashless society must figure out a way to protect their transaction data, acknowledging the risks of organizations collecting mass amounts of said data, which result in a reduction of personal privacy. Balancing individual privacy with data security is vital in the information age, especially considering the increasing risk of data breaches and exploitation.

In order to increase privacy in a cashless society, a few courses of action can be combined to produce a lasting and desirable result for users: A new kind of banking service that assigns randomized numbers to credit cards, the use of blockchain to monitor all transactions from individuals, and a campaign to educate and inform key stakeholders about security and privacy risks to provide the necessary tools and background knowledge to safeguard their own information before interaction with a foreign entity or other third parties (i.e. cybersecurity departments, IT technicians, etc). Blockchain and card number randomization are both susceptible to zero-day errors, bugs, and varied levels of social acceptance. This preliminary research draws on a systems analysis of cashless systems to identify and analyze a set of social and technical solutions to support a robust cashless system that protects users' privacy and maintains the security of the system.

The information found and analyzed will be beneficial by exposing weak points in current methods of data integrity and security. Learning about current and future methods of managing privacy and data security in the technological age would be helpful in creating preventative countermeasures. This study provides critical steps to prevent the loss of personal privacy in a cashless system.

***Index Terms*—cashless, society, privacy, security, data, system**

I. Introduction

Systems exist in a constant state of change, and their components must be updated in order to increase, or maintain, the ability to effectively accomplish a task and fulfill a purpose. The currency system is a complex one and requires a thorough analysis of its components, in order to operate at an acceptable level. A cashless system is an economic state where all transactions are performed without physical means of currency, such as coins or paper bills. For a cashless system, privacy is a crucial component in need of evaluation.

Increasing privacy is and will continue to be a necessary undertaking in a cashless society. A majority of users are unaware of what kind of data is being collected about them and how that data is being used. We thought the whole paper has realized the need for improving privacy, and we propose to do so with a three pronged solution. First, promoting proper education about data collection and privacy will help people realize the need for increased privacy. Second, a randomized credit card system will help prevent unwanted parties from collecting sensitive and personal information about people. Third, blockchain will prove to be a powerful authentication tool. Security will be drastically improved through the introduction of these three approaches. Users will have more knowledge about the systems they are using, hackers will have an exceedingly difficult time fooling the blockchain system, and data will be difficult to associate with specific people.

A cashless society poses risks for its members because all of their transactions will be tracked online. The members of said cashless society will have to figure out a way to protect their transaction data or risk the threat of organizations collecting mass amounts of data about them, which reduces personal privacy.

The remainder of the paper is organized as follows. Section II provides a relevant history of cashless transactions along with a useful definition of terms, in the context of this paper. In section III, we aim to highlight why our solutions must be considered in an evolving cashless society. Section IV proposes three solutions and depicts their implementation. Such changes will have impacts and implications, which are exemplified in section V. Then, section VI is designed to unveil potential problems that can occur between key system actors.

978-1-7281-7145-6/20/$31.00 ©2020 IEEE

Finally, we conclude the paper in section VII.

II. The Emerging Cashless Society

The idea of a cashless society includes using digitally-based technology to complete transactions, which can range from buying a soda at the convenience store to transferring large amounts of money from one account to another. Digital transactions can be completed using mobile applications, websites, credit or debit cards, and any other form of technology that comes to fruition in the future. Using technology to perform cashless transactions has become more prevalent in each successive decade since the 1940's [1].

A. Background of Cashless Transactions

Immediately after World War II, citizens began using credit cards. It was not until the 1980's that conventional point of sale transactions became widely used [2]. A point of sale transaction occurs when a customer swipes a card at a terminal to pay for some product or service. The terminal would read the magnetic strip and confirm the necessary account information to complete the transaction. Swiping cards with a magnetic strip is currently being phased out to adopt cards with chips physically installed in them. In the year 2000, PayPal was launched, and allowed users to transfer money online. The e-commerce website, eBay, uses PayPal to conduct transactions between users without having to involve personal bank account or credit card numbers.

In 2009, Bitcoin revolutionized the world of currency. This was an influential invention, because it was the first form of decentralized cryptocurrency. Anyone with an internet connection can obtain a bitcoin wallet, which contains a private key, used to make transactions and adjust the wallet's settings. Bitcoin exists outside the jurisdictions of traditional banking systems, which means that it cannot be ”banned” [1].

From 2010 to 2014 mobile payment apps such as Google Pay, Apple Pay, and Venmo launched. Mobile payments allow for users to make transactions using their mobile devices. Cell phones started out as devices which could only make voice calls, yet have become powerful tools capable of functionality comparable to desktop computers. Cell phones are becoming more powerful with an increasing amount of capabilities. With web-based applications available on mobile devices, online transactions have become easier and more convenient. By the year 2017, PayPal had 254 million customer accounts and had processed 7.6 billion payments. Mobile devices becoming more capable has contributed to this broad acceptance of the application [3].

B. Important Considerations

Privacy and security must be taken into consideration with the increasing use of cashless transactions. Privacy is the state or condition of being free from being observed or disturbed by other people. Privacy, in context of a cashless system, involves protection from involuntary collection and sorting of one's transaction information. Security is the state of being free from danger or threat. Privacy and security are important concerns in a cashless society. Any increase in convenience would be negated if people cannot secure their money and personal data.

III. Privacy and Security Concerns

A system is composed of elements, interconnections of the elements, and a function or purpose [4]. A cashless society is a system composed of entities such as standard users, governments, and banks. A cashless system provides a means of digital currency exchange. Privacy and security concerns within a cashless system are abundant and must be addressed.

A. The Collection of Data

In a completely cashless society, and in today's age, every transaction one makes on their credit card is kept in the corresponding retailer's database. The information collected from customer transactions are used for accounting and tax purposes by all businesses, but many of them collect mass data about people. For example, when a person buys some product from Target, the store keeps a record of what that card has purchased [5]. This record is linked to that specific card and whatever other information Target can gather about that customer. As a result, people are unknowingly being exploited for the information they may not realize they are giving out. The desired level of privacy would include a user to avoid having their transactions be collected and unethically used by businesses and corporations.

Any kind of obtainable data can be stored and sold if the quantity and quality of data is useful for business or government applications. Data brokers collect and sell personal information about people. This information is often collected about people without their knowledge nor explicit consent [5]. In this day and age, it's difficult to prevent data brokers from gaining information about individuals. Almost everything people do is tracked in some way and used for another purpose. People can view this as an invasion of privacy. It is important to note that our daily lives are becoming less private.

B. Ethical Considerations

Securing private data is especially important in locations where governments and their agencies use data to make conclusions about citizens. Individuals can be associated with criminals in government databases, because they meet certain criteria. Government agencies use data about people in order to find criminals [5]. If criminals typically buy certain products over a specific period of time, machine learning algorithms will be able to detect this. If a non-criminal civilian purchases a similar product over the same time period, they could be identified as a potential criminal. If the government agency is prevented from gaining access to large amounts of transaction data, innocent people could avoid being associated with criminals [6]. However, associations don't stop at criminal activity. The purchasing of certain products with a particular frequency could be used by insurance companies and banks to identify people with medical conditions or who are more likely to default on a loan.

This complex scenario of what to do with all the data gives rise to tensions between ethics and the furthering of business or governmental objectives. Solutions must be considered and implemented in order to mitigate privacy concerns.

IV. Solutions Analysis

Solving the problem of decreased privacy and security in a cashless society requires implementing new technological methods and providing valuable information to the public.

A. Randomized Credit Card Numbers

In order to prevent stores and businesses from collecting information about their customers, randomized card numbers can be used. If a customer using the randomized card system purchases groceries from a store, the items bought will be linked to a certain card number. If the customer with the same card returns to the same store on another day, the purchase will be linked to a different card number than the previous day. Figure 1 depicts the difference between using a standard credit card and a randomized card, in relation to a store's database. The database saves the real card number for standard credit cards, and a different number for the randomized one.

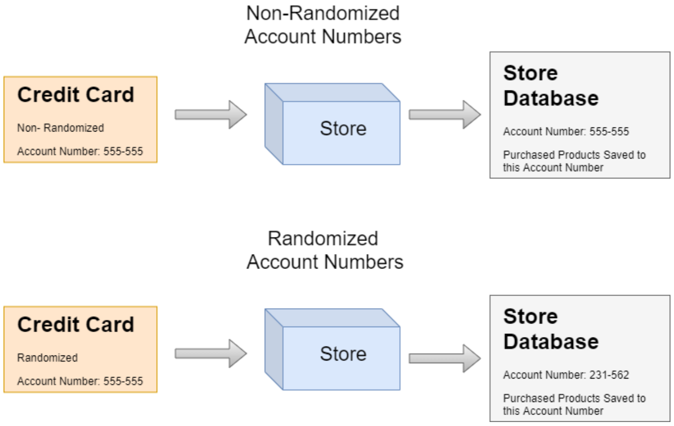

Figure 1. The Randomized Credit Card

The randomized card system would behave similar to a VPN (Virtual Private Network) used for Wi-Fi connectivity. When a mobile device is searching to connect to a Wi-Fi signal, without using VPN, it sends out it's real IP address (Internet Protocol address) [7]. On the other hand, a VPN allows for the mobile device to send out a proxy IP address, then authenticate the network, then give out it's real IP address. However, the randomized credit cards will operate slightly differently than VPN.

The randomized credit card system will consist of a primary account number that is linked to randomized card numbers that are linked to individual transactions. When an account holder wants to check their transaction history, they can log into their bank's app or website and check their purchases in real time.

B. Blockchain

Another system that all levels of government will need to set in place will be a nationalized blockchain network, which will handle tracking transactions in a secure and private manner. According to Melanie Swan's Blockchain: Blueprint for a New Economy, blockchain operates as a public ledger of all transactions [8]. The blockchain will have complete information related to each transaction and the data of each person involved in said transaction. Such technology is more secure than other record-keeping systems. Blockchain's ability to track in real-time allows for the elimination of error handling, which also allows for improved traceability.

Such a feat would first need to be built by the collective efforts of developers, engineers and designers. Regulations and operators/maintainers can be established through lawmakers initially passing laws that address who will be operating and maintaining the secure blockchain network and moving the financial aspects of life to the network.

C. Implementation

In order for the public to accept a randomized credit card system, users must either have incentive to switch accounts or no need to switch at all.

Incentives to switch bank accounts could be influenced by a publicly accepted need for increased privacy. If the randomized credit card system is made into a standard, then every bank can adopt and implement it for their users. This task will not be simple but would provide the best possible outcome for users, which would be more privacy and minimal hassle. Regarding blockchain, the previously listed features will provide increased privacy and security to users to those living and working in the United States.

To successfully roll out such changes to the modern financial system, education and public outreach will be essential. Focusing on the privacy and security aspects concerning a cashless society, this stage is aimed to prepare future members for a life after cash. A public awareness campaign would emphasize gaining and improving upon knowledge and understanding of current privacy laws and other practices regarding finances. This policy-oriented approach would primarily focus on preemptive privacy and security while increasing technological literacy throughout the population. Preemptive privacy can be defined as client-side decisions which have a positive effect on the level of privacy and/or security of their data (before implementing strategies like blockchain and other forms of encryption). In 2019, there were 1,473 data breaches, with 164,683,455 records containing sensitive data released [9]. Although this statistic is smaller than the previous year, it is still important to highlight the importance of safeguarding personal data and the reality of vulnerabilities in the security of private information. By instilling more power and autonomy into the society first, there will be increased flow of information, which will dispel most of the uncertainty and distrust in a cashless system. According to Donella Meadows, one of the root causes of system malfunctions is a lack of or disturbance in information flow [10]. By providing a source of knowledge and transparency to those who may not have as much experience with electronic forms of payment, this system would teach people how to properly manage their own privacy, while also maintaining current privacy and security measures. By sharing the responsibility with the user, companies and other entities with greater power can provide greater focus towards the products or services they provide. Minimizing human error will allow for more effort to be put towards more serious cybersecurity risks and issues. Although large companies will most likely experience a decrease in data acquisition and analytics, more attention can be directed towards bolstering current cybersecurity measures and protecting one of their most important economic assets: the customer. Large organizations handling, storing, and managing transactions (stores and banks) would benefit from their users responsibly managing their privacy and security. Data breaches cost companies millions of dollars to deal with. In 2019, the average cost of a data breach to a United States-based company was $8.19 billion [11]. By relying more on the responsibility of users, large companies entrusted with valuable data will ideally be able to pay greater attention to their own security risks and loopholes within databases and firewalls.

V. Predictive Analysis

A cashless system is composed of many different elements. Each element may respond differently to changes. Analyzing potential solutions to a problem can give helpful insight about how their application will affect the system.

A. Using Blockchain

Currently, physical vaults that house cash in consumer banks and federal banks face the threats of robbery and damage. With a blockchain network, there would exist secure, encrypted confirmations of money-flow. There would be no worry of intrusion, due to the level of security in place, combining manpower and machine.

B. Using a Randomized Card System

Credit cards are vulnerable to skimming devices, which can be strategically placed on real-working scanners and serve to "skim" and save sensitive data that credit cards are associated with. A randomized card system will help alleviate this issue, by granting a randomized credit card number to the swiped or inserted card, adding an additional security measure, which will in turn lift fraud-related issues that banks deal with on a daily basis.

C. Social Responsibility and Awareness

Entrusting the public to learn about and manage their own financial privacy is vital concerning the future development and popularity of cashless forms of payment. With the trend towards a completely cashless society, it is important for users to have the knowledge, experience, and logical understanding needed to safeguard their own information.

Encouraging technological literacy through educational, public outreach campaigns would alleviate some of the burden carried by technology companies and service providers. Awareness of the inherent risks involved in a cashless society would reduce many ignorance-induced problems people experience regarding the security and privacy of their financial and personal data.

D. The Technological Progression

With a credit card randomization system and a nationalized blockchain network, user privacy and security will increase. Rather than replacing current means of financial transaction, such an action would complement those daily spending activities and habits. As transactions are made, and any data associated with said transactions, will be kept secure either through randomized credit card numbers or the blockchain's improved real-time traceability.

E. Implications

An economic implication of establishing a nationalized blockchain network is that the demand for human-operated labor in the financial institutions will likely decrease, resulting in a societal shift to computational-based interactions [12]. This is a likely scenario, as the system will be running checks on every transaction and will be able to send, receive, and process messages.

For the credit card randomizer, a legal implication would be that the advanced well-maintained technology would decrease the amount of fraudulent transactions, saving the time of credit card companies, banks, and ultimately law professionals.

F. Fitting into Society

It is normal for a society to fear something that it does not understand or that seems foreign to their traditions. Initially, there may be disapproval of a cashless society from both the political right and left. If the situation surrounding Facebook and the United Kingdom based political consulting firm, Cambridge Analytica, has taught the world anything, it is that lawsuits may be the key to obtaining tighter data privacy in the United States. Facebook's suspension of Cambridge Analytica was a scandal in which the consulting firm improperly acquired the data of 50 million Facebook users in 2014-2015, which was then used in Donald Trump's presidential campaign [13] of that time.

Society will quickly realize this new technology is necessary for their everyday lives, as each day that goes by without it, the more data corporations are able to collect and the more control they will have over their lives.

VI. Further Systemic Concerns

Key system actors, in a cashless society, will compete to advance their own interests. In the context of systems thinking, an archetype is a 'common pattern of problematic behavior' [4]. Problems are relative to which groups of people, or actors, they affect.

A. Relevant Archetype

Policy resistance is an archetype which consists of solutions that fail. For policy resistance to occur, actors in the system must be primarily concerned with only one interest, such as money or power [4]. When the actor's interest is behaving in an undesirable way, they make changes to benefit that one aspect of the system.

The system failure can be attributed to a lack of concern for the rest of the system. A single change can cause a variety of externalities to occur in the rest of the system. A place in a systems structure that can cause large changes to the rest of the system is called a leverage point [14]. Leverage points are effective places to implement solutions because of their tendencies to produce large changes with relatively minimal input [4].

B. Historical Example

A common example of policy resistance can be found in the history of ciphers (code makers) and code breakers. Some of the oldest ciphers date back to 400 BC, where the Greeks used a special method of encoding called scytale [15]. Scytale was extremely useful for hiding the meaning of messages from enemies. Once the enemies figured out how to break the code, they gained the advantage. Each actor in this system of encoding and decoding is forced to work harder and harder to achieve their objective. Every time a cipher fails, it produces a non-result where there's no means of encryption.

C. Breakdown of Key Actors

Large technology companies are concerned with having high profits, which can be increased through more data collection. Data brokers also want high data collection to increase their profits from sales. However, consumers want data collection to be lowered in order to increase their privacy. Then, the government falls somewhere in the middle between high and low data collection, and balancing corporate and citizen needs. Government agencies also buy data from data brokers [16], yet they also serve to protect citizens' privacy to a certain extent.

If consumers take action and limit their data collection through means of becoming educated about privacy and using emerging technologies that promote privacy, they will alter the amount of data collection for other actors. Once there is a shortage of data, large technology companies and data brokers will be forced to find ways to increase it again. Such methods could include large technology companies making premium and standard models of products. They will either make money by selling a more expensive product or collect more data off the cheaper model.

D. The Way Out

Regardless of the actual outcomes of a cashless society, policy resistance is a serious problem to take into consideration. The primary actors involved in data collection have the power to use leverage points to make changes to the whole system. According to Meadows, the way out of policy resistance is to bring actors together in a mutually beneficial way [4]. The art of compromise is delicate and often depends upon bargaining power. The large technology companies have capital, consumers have data and money to spend, and the government has the power to make and enforce policies.

Our group believes the most likely course of action will include the key actors participating in a long-term push and pull of more versus less data collection. A combined effort between the actors is unlikely. Each actor has their own goals and reasoning for wanting certain amounts of data collection. This is not to say a combined solution is impossible, just unlikely.

VII. Conclusion

A cashless society poses risks for its members because data and metadata about their transactions are being collected and used. The members of said cashless society will have to figure out a way to protect their data in order to increase their privacy.

Our group has found the idea of a cashless society to involve many systemic complexities. Within the complex system, opportunities arise to implement solutions to privacy and security problems. The various actors in said system have different desires and will respond in unique ways to changes made.

Sometimes the best solution to a problem is the culmination of multiple approaches. Spreading information to the general public helps people learn about the systems they are using and allows for them to make informed decisions. Blockchain helps promote privacy and security through its authentication process. Randomized credit cards help users keep their account numbers private. All three approaches are effective ways of adapting to a dynamic currency system.

References

[1] "Bitcoin - Open Source P2P Money." n.d. Accessed December 12, 2019. https://bitcoin.org/en/.

[2] Wolters, Timothy. "'Carry Your Credit in Your Pocket': The Early History of the Credit Card at Bank of America and Chase Manhattan." Enterprise & Society 1.2 (2000): 315-54. Print.

[3] Mercer, Christina. n.d. "History of PayPal: 1998 to Now." Techworld. Accessed December 12, 2019. https://www.techworld.com/picture-gallery/business/history-of-paypal-1998-now-3630386/.

[4] Meadows, Donella H., and Diana Wright. Thinking in Systems: a Primer. Chelsea Green Publishing, 2015.

[5] Andrew Ferguson, The rise of big data policing: surveillance, race, and the future of law enforcement," New York; New York University Press, 2017.

[6] "The Rise of Big Data Policing — TechCrunch." n.d. Accessed February 5, 2020. https://techcrunch.com/2017/10/22/the-rise-of-big-data-policing/.

[7] Symanovich, Steve. "What Is a VPN?" Official Site, us.norton.com/internetsecurity-privacy-what-is-a-vpn.html.

[8] Swan, M. (2015). Blockchain: Blueprint for a New Economy. Sebastopol, CA: OReilly Media, Inc.

[9] 2019 Data Breaches - Identity Theft Resource Center. (2020). Retrieved 27 March 2020, from https://www.idtheftcenter.org/2019-data-breaches/

[10] "Leverage Points: Places To Intervene In A System." The Academy for Systems Change. N. p., 2020. Web. 3 Feb. 2020.

[11] "What's New In The 2019 Cost Of A Data Breach Report." Security Intelligence. N. p., 2020. Web. 6 Feb. 2020.

[12] Arthur, W. (2018, March 23). Lawsuits may be key to tighter US data privacy rules. Retrieved March 26, 2020, from https://dailybrief.oxan.com/Analysis/DB230635/Lawsuits-may-be-key-to-tighter-US-data-privacy-rules

[13] Arthur, W. (2018, March 23). Lawsuits may be key to tighter US data privacy rules. Retrieved March 26, 2020, from https://dailybrief.oxan.com/Analysis/DB230635/Lawsuits-may-be-key-to-tighter-US-data-privacy-rules

[14] “Leverage Points: Places to Intervene in a System.” The Academy for Systems Change, donellameadows.org/archives/leverage-points-places-to-intervene-in-a-system/.

[15] Singh, Simon. The Code Book: the Secrets behind Codebreaking. Ember, 2016.

[16] Marwick, Alice E. “How Your Data Are Being Deeply Mined.” The New York Review of Books, www.nybooks.com/articles/2014/01/09/how-your-data-are-being-deeply-mined/.