WHAT’S IN YOUR DIGITAL WALLET?
IS IT YOUR IDENTITY AND HAVE YOU LOST YOUR PERSONHOOD?

Thesis
submitted to the Faculty of
The School of Continuing Studies
and of
The Graduate School of Arts and Sciences
in partial fulfillment of the requirements for the
degree of
Master of Arts
in Liberal Studies

By
Lori Santamorena, B.S and B.A.

Georgetown University
Washington, D.C.
February 18, 2016
WHAT’S IN YOUR DIGITAL WALLET?
IS IT YOUR IDENTITY AND HAVE YOU LOST YOUR PERSONHOOD?

Lori Santamorena, B.S. and B.A.

MALS Mentor: Douglas M. McCabe, Ph.D.

ABSTRACT

Do the devices we use redefine what it is like to be human? This thesis looks at whether digital wallets are determining our identity and deemphasizing personhood, leading to ethical and social maladies.

The foundational concept of this thesis is based on Jaron Lanier’s *Your Are Not a Gadget: A Manifesto*. Lanier argues that “certain specific popular internet designs of the moment - not the internet as a whole - tend to pull us into life patterns that gradually degrade the ways in which each of us exists as an individual.”

The ethical malady of privacy assessed digital wallets and their relationship with freedom and autonomy across generations. Digital wallets and data collection were compared to physical wallets. The digital divide as an ethical malady examined the potential gap between those who have ready access to digital wallets compared to those who do not. Digital wallets’ impact on class systems contemplated the potential to raise economic and social inequalities between groups of people. Regulations and standards applicable to digital wallets were studied. Applying the concept of paradigm shift to digital wallets was also considered.

Using a digital wallet instead of a physical wallet is an individual choice. You are not being forced to use a digital wallet. You control the destiny of your personhood, those
qualities that confer your distinct individuality. Do you want your identity in your back pocket or flying around on a cloud or on the internet? As technology advances, is the digital wallet destined to become the virtual representation of a person, redefining what it means to be human? Your identity is tangible, is your digital wallet?
ACKNOWLEDGMENTS

This is to express my sincere appreciation to: Professor Douglas McCabe, my thesis mentor; Professor Gladys White, for the idea; Anne Ridder, for her support; and my dear sister, Catherine Moritz. The views expressed are those of the author only.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>ii</td>
</tr>
<tr>
<td>ACKNOWLEDGMENTS</td>
<td>iv</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>CHAPTER 1 ETHICS AND COMPUTERS</td>
<td>5</td>
</tr>
<tr>
<td>CHAPTER 2 WHAT IS A DIGITAL WALLET?</td>
<td>17</td>
</tr>
<tr>
<td>CHAPTER 3 ETHICAL AND SOCIAL MALADIES</td>
<td>29</td>
</tr>
<tr>
<td>CHAPTER 4 REGULATIONS, STANDARDS, AND ROLES</td>
<td>46</td>
</tr>
<tr>
<td>CHAPTER 5 PARADIGM SHIFT?</td>
<td>65</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>82</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>85</td>
</tr>
</tbody>
</table>
INTRODUCTION: OVERVIEW OF THESIS AND ANALYTICAL APPROACH

Do the devices we use redefine what it is like to be human?

This thesis will describe the evolving ethical culture around the use of digital wallets and what it means to be human.

As our wallets become e-wallets housed somewhere out on the Internet rather than in our back-pockets, and as our public institutions, businesses, and even cultural institutions find homes online, the confidentiality of our communications, papers, and information is at risk of compromise.¹

Specifically, this thesis will take a closer look at whether digital wallets are determining our identity and deemphasizing personhood, leading to ethical and social maladies.

Personhood, as described by Martha Farah and Andrea Heberlein in “Personhood and Neuroscience: Naturalizing or Nihilating” is generally defined as “the state or condition of being a person, especially having those qualities that confer distinct individuality.” The authors explain that the earliest explicit definition of personhood came from the sixth-century philosopher Boethius who equated a person with “an individual substance of a rational nature.” Judeo-Christian theology offers a different perspective on personhood, emphasizing a person’s relationships, including relationships with other persons and God. According to this view, as expanded by Farah and

---

Heberlein, it is the “participation in these relationships that endows an individual with personhood.”² Basically, it is your individuality or uniqueness.

This thesis will explore ethical principles and information technology. A person’s right to privacy and recognizing that individual as an autonomous human being will be considered.³ The principle of justice, and whether digital wallets accentuate the digital divide, will also be contemplated.

The foundational concept of this thesis will be based on Jaron Lanier’s *You Are Not a Gadget: A Manifesto*. Lanier argues that “certain specific popular internet designs of the moment - not the internet as a whole - tend to pull us into life patterns that gradually degrade the ways in which each of us exists as an individual.”⁴

Other works will support this research, including James Moor, “Towards a Theory of Privacy in the Information Age.” Moor writes as follows:

Using the core value framework privacy can be grounded instrumentally and intrinsically- instrumentally, as a support of all core values, and, intrinsically as an expression of security… Privacy, as an expression of security, is a critical, interlocking member in our systems of values in our increasingly computerized culture.⁵

---


The propositions raised by Norbert Wiener’s foundational work in computer ethics, *The Human Use of Human Beings: Cybernetics and Society*, will also be considered, including an account of the purpose of life and four principles of justice.  

Using the work of Jaron Lanier, the core argument of this thesis is to explore whether digital wallets deemphasize personhood, and the intrinsic value of an individual’s unique internal experience and creativity. To accomplish this, digital wallets will be studied to assess whether their existence leads to ethical and social maladies. The ethical malady of privacy will be examined, including its relationship with freedom, and how privacy is viewed across generations. The extent of intelligence and range of how much “they” know about you, and is that a much wider range with a digital wallet, will be studied. The digital divide as an ethical malady will be examined to evaluate the potential gap between those who have ready access to use digital wallets compared to those who do not.

This paper will consider the impact of digital wallets on class systems and the potential to raise economic and social inequalities between groups of persons. The inequalities that will be studied include whether the same benefits exist for people choosing to use or not use a digital wallet, or whether they are disadvantaged.

The existence of standards and regulations, and the government’s responsibility, will also be studied. Now that the contents of your digital wallet are not in your back pocket, does this change the potential risks consumers may be confronted with, and what, 

---

6 Norbert Wiener, *The Human Use of Human Beings: Cybernetics and Society* (New York: Houghton Miflin, 1954). Norbert Wiener was a professor of mathematics at Massachusetts Institute of Technology in the 1940s-50s, and invented the field of cybernetics. He is credited with inspiring a generation of scientists to think of computer technology as a means to extend human capabilities.
if any, safeguards exist. If a consumer’s spending patterns and credit history are now available in one place, is the consumer aware that this information is being accumulated? Is the public being protected from nefarious individuals and marketers who have our consumption data? Finally, is there evidence of a paradigm shift in payment mechanisms from cash to credit cards to digital wallets?

As technology advances, is the digital wallet destined to become the virtual representation of a person? This thesis will evaluate whether digital wallets de-emphasize personhood by redefining what it means to be human. My identity is tangible; is my digital wallet?
CHAPTER 1: ETHICS AND COMPUTERS

This chapter explores the evolving ethical culture around computers and information technology. The foundational concept is based on Jaron Lanier’s *You Are Not a Gadget: A Manifesto*. The propositions raised by Norbert Wiener’s pioneering work in computer ethics, *The Human Use of Human Beings: Cybernetics and Society* are considered, including his account of the purpose of life and four principles of justice. James Moor’s and Terrell Ward Bynum’s essays on computer ethics will also be explored.

In *You Are Not A Gadget: A Manifesto*, Lanier argues as follows:

Certain specific, popular internet designs of the moment – not the internet as a whole - tend to pull us into life patterns that gradually degrade the ways in which each of us exists as an individual. These unfortunate designs are more oriented towards treating people as relays in a global brain. Deemphasizing personhood, and the intrinsic value of an individual’s unique internal experience and creativity, leads to all sorts of maladies ... While the core argument might be described as “spiritual,” there are also profound political and economic implications.¹

Lanier traces the deterioration that he believes transformed our lives for worse with the rise of the Web 2.0 design in the late 1990s, rather than the internet itself. Web 2.0 refers to the transition from static HTML pages to World Wide Web pages that focus on user collaboration, and the sharing of user-generated content.

Lanier explains that these designs value the information content of the web over individuals. “It became fashionable to aggregate the expressions of people into

¹ Lanier, *You Are Not A Gadget: A Manifesto*, x.
dehumanized data. There are so many things wrong with this that it takes a whole book to summarize them.” 2

Analyzing Wiener’s approach to information ethics issues and the effect of information technology on human values, human nature, and society, provides an ethical basis for the purpose of human life and a foundation for thinking about digital wallets in later chapters.

Norbert Weiner is considered the first thinker on what is now called computer ethics. Because of the applicability of his ideas and methods to a range of information technology, “information ethics” was name given to the field of ethics he founded. Computer ethics is considered a subfield of information ethics.

While Wiener did not live to see the internet, he viewed the integration of information and communication technology (ICT) into society as transformational, leading to the remaking of society to the “second industrial revolution” and the “automatic age” destined to affect every walk of life. Wiener envisions that “we are here in the presence of another social potentially of unheard of importance for good or evil.” 3

In *The Human Use of Human Beings*, Wiener examines ways in which information and communication technology could affect key human values like life,

---


health, work, wealth, knowledge, ability, creativity, happiness, democracy, freedom, peace, and security.4

Wiener starts with a good human life where “great human values” are realized, one in which the “creative and flexible information processing potential of the human sensorium enables humans to reach their full promise in variety and possibility of action.” He adopts “great principles of justice” on which a society should be built that would maximize a person’s ability to flourish through variety and flexibility of human action. Wiener’s ethical principles are as follows:

The Principle of Freedom - Justice requires the liberty of each human being to develop in his freedom the full measure of the human possibilities embodied in him.

The Principle of Equality - Justice requires the equality by which what is just for A and B remains just when the positions of A and B are interchanged.

The Principle of Benevolence - Justice requires a good will between man and man that knows no limits short of those of humanity itself.

Principle of Minimum Infringement of Freedom - What compulsion the very existence of the community and the state may demand must be exercised in such a way as to produce no unnecessary infringement of freedom.5

Wiener introduces a fourth principle of minimum infringement to limit society’s negative impact on freedom. He views people as fundamentally social beings who reach their full potential only by actively participating in communities of similar beings,


and that society is essential to a good human life. But Wiener wrote that an oppressive society could limit freedom.

Conceptually, one can look at modern day programs, such as the Software Engineering Ethics Research Institute at East Tennessee State University, and see a connection to Wiener’s vision. Their program focuses attention on professional responsibility to advance the professionalization and ethical maturation of computing practitioners. Its founder, Professor Donald Gotterbarn, developed a computer program to assist individual companies and organizations prepare ethical stakeholder analyses to determine likely ethical impacts of software development projects.6

Computer ethics essayist Terrell Ward Bynum asserts that Wiener’s methodology for analyzing and solving computer ethics questions assimilated new ethical judgments and new cases into the existing cluster of laws, rules, practices and principles that govern human behavior.

Using Wiener’s foundation, Bynum construes the following five steps based on Wiener’s methodology as follows:

Step One: Identify an ethical question or case regarding the integration of ICT into society.

Step Two: Clarify any ambiguous concepts or rules that may apply to the case in question.

Step Three: If possible, apply existing policies (principles, laws, rules, practices) that govern human behavior in the given society. Use precedent and traditional interpretation in such a way as to assimilate the new case or policy into the existing set of social policies and practices.

Step Four: If precedent and existing traditions are insufficient to settle the question or deal with the case, revise the old policies or create new ones, using “the great principles of justice” and the purpose of a human life to guide the effort.

Step Five: Answer the question or deal with the case using the revised or enriched policies.\(^7\)

Wiener and Lanier appear to share similar thinking in their approach to human beings, personhood, and the information age even though their writings are over fifty years apart.

Lanier describes the challenges posed by the new age internet and values on personhood. On the idea that information rather than an individual wants to be free, Lanier observes as follows:

And the problem with that is that it anthropomorphizes information. Information doesn’t deserve to be free. It is an abstract tool; a useful fantasy, a nothing. It is non-existent until and unless a person experiences it in a useful way. What we have done in the last decade is give information more rights than are given to people. If you express yourself on the internet, what you say will be copied, mashed up, anonymized, analyzed, and turned into bricks in someone else’s fortress to support an advertising scheme. However, the information, the abstraction, that represents you is protected within that fortress and is absolutely sacrosanct, the new holy of holies. You never see it and are not allowed to touch it. This is exactly the wrong set of values... The idea that information is alive in its own right was a metaphysical claim made by people who hope to become immortal by being uploaded into a computer someday. It is part of what should be understood as a new religion. That might sound like an extreme claim, but go visit any computer science lab and you will find books about “the Singularity,” which is the supposed future event when the blessed uploading is to take place. A weird cult in the world of technology has done to the culture at large.\(^8\)

---

\(^7\) Bynum, “Norbert Weiner’s Foundation of Computer Ethics,” 3-4.

Like Lanier, Wiener talks about a person’s ability to flourish, not the technology. Wiener’s Principle of Freedom provides that “justice requires the liberty of each human being to develop in his freedom the full measure of the human possibilities embodied in him.” If freedom is another way to say autonomy, does certain technology unnecessarily infringe on my personhood?

Wiener reflects that the “defining goal of computer ethics, then, is to advance and facilitate the good consequences of ICT while preventing or minimizing the harmful ones.”

Is it feasible to apply Wiener’s thinking on assimilating new ethical judgments and cases into already existing, ethically acceptable laws, rules, and practices? In any given society, there is a network of existing practices, laws, rules, and principles that govern human behavior. Wiener believes that a better world would be created with information and computers, but action by a community would be needed to keep the values. Wiener predicts that computers would be “hooked up to artificial sense organs and would replace the human blue collar worker, and the unscrupulous factory owner would get rich at the expense of the blue collar worker.” He suggests that union leaders, business managers, and public policy makers should plan ahead and develop ways to deal with these problems before they happen.

Do computers and digital wallets raise special ethical issues that Wiener may not have envisioned in developing his approach to ICT? James Moor takes a divergent

---

10 Ibid., 5.
approach to Wiener. What Moor sees as revolutionary about computers is “logical malleability.” Moor explains that computers can be “shaped and molded to do any activity that can be characterized in terms of inputs, outputs, and connecting logical operations.” Moor saw the computer revolution as occurring in two stages. The introduction stage of computer technology has been occurring during the last several decades. The second stage, which Moor refers to as the permeation stage, is one in which computer technology will become an integral part of institutions throughout our society. Potentially, as this is integrated into everyday human activities and into social institutions, Moor thinks many human activities and social institution will be transformed by computer technology and this transforming effect of computerization will raise a wide of issues for computer ethics.11

Moor illustrates the transformational effect of computer technology on financial institutions with the advent of electronic funds transfers and payments. Moor observes that it is not how well computers count money but rather what is money. As a computer records or electronic impulses replace money, what opportunities and values are lost or gained when money becomes intangible.12 As explored in later chapters, digital wallets raise similar issues because a wallet acts as a conduit to store value.

---


Moor writes as follows:

The ethical evaluation of a given policy requires the evaluation of the consequences of that policy and often the consequences of the policy compared with the consequences of other possible policies. If actions involving computers had no harmful consequences, policies would not be needed. However, conventional consequentialism seems to be insensitive to issues of justice.\(^\text{13}\)

Moor believes there may be a unifying ethical theory that takes into account the consequences of policies while at the same time making sure these policies are constrained by principles of justice.\(^\text{14}\)

He proposes that computers create new possibilities for action. These possibilities give rise to ethical and social issues that are not easily anticipated and that are not always able to be subsumed under existing policies and laws, resulting in “policy vacuums.” Initially, it might appear that existing policies can be extended or framed as new policies to fill vacuums. But Moor explains that this may not always work because policy vacuums are often accompanied by “conceptual vacuums” or “muddles.” Moor believes what is needed in these cases is a coherent conceptual framework to formulate a policy for action.\(^\text{15}\)

Moor’s reflection on a cashless society illustrates this point as follows:

Monetary transactions were grounded in gold. Then the gold standard was dropped and the paper bills became the money. To have money was to have the paper, presumably backed by the good faith and trust in the government. Now paper has been augmented with credit cards and debit cards that can read by computers. Of course, these cards are not real money because one can always


\(^{14}\) Ibid., 66.

\(^{15}\) Moor, “What is Computer Ethics,” 266-275.
exchange the credits for paper money. But it is likely that the use of paper money will decrease and the electronic token on the cards or in a bank’s computer will become the money. Some cards now have chips embedded in them so they can be loaded with electronic money which is then transferred as information to a merchant at the point of sale. We are headed for a cashless society. Monetary transactions are increasingly grounded in information. Money may come to be conceived as an elaborate computable function among people. In the computer age the concept of money is becoming informationally enriched.16

Informational enrichment that may affect ethical and legal practices and concepts applied to digital wallets and electronic commerce will be discussed in subsequent chapters.

Like Wiener, Moor identifies core values (life, happiness, ability, freedom, knowledge, resources, and security) that provide standards to evaluate the rationality of our actions and policies.

Moor highlights the special ethical challenges information raises. As information is computerized it is “greased” to slide easily due to speed and convenience, potentially leading to improper exposure of information. Moor explains that the “greasing of information allows other computers to capture and manipulate information in ways we do not expect.”17

Further complicating the thinking on applying computer ethics that potentially could be applied to information rich digital wallets is that computers have reframed the privacy debate. Moor notes that privacy is not a core value, and that the concept of


privacy has a cultural aspect that goes beyond the core values. Some cultures may value privacy, and others do not. According to Moor, “privacy is instrumental in support of core values. It is the expression of a core value, without it we cannot flourish.”

Moor contends that in a highly computerized culture in which lots of information is greased, it is almost inevitable that privacy will emerge as an expression of the core value security. He believes it is then a plausible candidate for an intrinsic good in the context of a highly populated, computerized society.

Moor notes that “using a core value framework privacy can be grounded both instrumentally and intrinsically to support core values and as an expression of security. Individuals and societies that are not secure do not flourish and do not exist for long.” Moor believes as follows:

It is imperative that we create zones of privacy that allow citizens to rationally plan their lives without fear. The zones of privacy will contain private situations with different kinds and levels of access for different individuals. It is important to think of privacy in terms of control and restricted accounts, because this concept encourages informed consent and fosters development of practical, fine grained and sensitive polices for protecting privacy when it is not.

Computers and technology have transformed the debate on privacy and the need for computer-specific Fourth Amendment rules. Moor notes that privacy has become so “informationally enriched” that it refers to “informational privacy.” Another debate has

---

18 Ibid., 29.

19 Ibid., 29-30.
surfaced, this one having to do with the possible recognition of the use of the internet as a “human right.” 20

Moor also references ethics author Deborah Johnson’s perspective on privacy and autonomy. Assuming autonomy is intrinsically valuable, and privacy is a necessary condition for autonomy, Johnson writes that we have a strong and attractive claim that “privacy is necessary for intrinsic good and if privacy is not an intrinsic good itself it is the next best thing.” 21

Lanier offers optimism, writing how the internet transformed our lives for the better as follows:

The answer is different in different parts of the world. In the industrialized world, the rise of the Web has happily demonstrated that vast numbers of people are interested in being expressive to each other and the world at large. This is something that I and my colleagues used to boldly predict, but we were often shouted down, as the mainstream opinion during the age of television’s dominance was that people were mostly passive consumers who could not be expected to express themselves. In the developing world, the Internet, along with mobile phones, has had an even more dramatic effect, empowering vast classes of people in new ways by allowing them to coordinate with each other. That has been a very good thing for the most part, though it has also enabled militants and other bad actors. 22

---


As technology advances, is the digital wallet destined to become the virtual representation of a person, de-emphasizing personhood and redefining what it means to be human? Your identity is tangible, is your digital wallet?
CHAPTER 2: WHAT IS A DIGITAL WALLET?

Physical and digital wallets are explored in this chapter.

Merriam-Webster Dictionary defines a wallet as follows:

wallet
noun wal·let \ˈwä-lat\ 
: a small folding case that holds paper money, credit cards, etc.
Full Definition of WALLET
1 
: a bag for carrying miscellaneous articles while traveling
2 
a : a folding pocketbook with compartments for personal papers and usually unfolded paper money; also : billfold
b : a container that resembles a money wallet: as (1) : a usually flexible folding case fitted for carrying specific items (as tools or fishing flies) (2) : folder

Physical wallets are typically used to store things of value. Wallets date back to Ancient Greece and Rome, and were used to hold food. During the Renaissance period wallets were used as a leather sack with a drawstring to hold paper currency, coins, and miscellaneous paperwork. In the 1690s when paper currency was introduced, they began making wallet out of leather, and included a place to store calling cards and other forms of identification. By the 1800’s, Americans workers began to attach leather pouches to their belts. These leather pouches would become the prototype wallet until the mid-20th century when the leather billfold was introduced.

The contents of your wallet may tell us something about you as a person. The things you store in a wallet may represent your judgment of what may be important in

---


your life, its worth, or usefulness. It may represent financial security to certain people, along with purchasing power and prosperity. For some people their wallet contains their life story, their identity. The size of a wallet may tip you off about a person’s gender. A widely held belief is that the bigger a woman’s purse, the more she will cram into it, and the same goes for her wallet. She may keep her membership cards, coupons, receipts, business cards, credit and bank cards, photos, metro transit card, and anything else she can fit, into her wallet.

Digital commerce has transformed the concept of a wallet. Unlike a physical wallet, there is no standard definition of “digital wallet.” For purposes of this thesis, we will refer to a digital wallet or a mobile digital wallet or mobile wallet interchangeably.

How a digital wallet works, and its interaction with the digital wallet user, may help inform thinking about its impact on personhood. As Lanier writes, “The most important thing about technology is how it changes people.” 3

A digital wallet is a software application that enables users to digitally store money, payments credentials and more, in order to implement various types of cashless transactions. A digital wallet has been described as a way to pay for something with a device such as a computer or mobile phone. It is able to take the functions of a physical wallet, with all of its contents and behaviors, and integrate it into the digital device.4


The software application stored on a mobile phone that manages and initiates payments is generally referred to as a mobile digital wallet or a mobile wallet. It is funded by a credit or debit card, prepaid account, bank account, or charged to a mobile phone bill.

The “digitized valuables” stored in a mobile wallet can be represented in many different forms. They may take the form of a number (like on a credit card or a password), a digital certificate, a mobile phone readable bar code referred to as a Quick Response Code (QR Code), an image of the owner, or something else. These representations are linked to the digital wallet owner’s sensitive personal information. Digital wallets provide valuable access to this information, but may require stronger protection and security.5

The same or similar objects kept in a physical wallet may be more neatly stored and grouped on a digital wallet, eliminating the clutter. A digital wallet may be able to provide additional functions and benefits such as virtually unlimited storage, location, awareness, and quick sorting or searching of its contents. Doing away with the paper receipts, business cards, and other paper artifacts, and the potential for optimizing or eliminating trips even benefits the environment. Does this make a digital wallet a more compelling replacement for a physical wallet? 6


There may be trade-offs to using a digital wallet. Unlike a physical wallet, a digital wallet owner may have the perception of autonomy over their wallet, but it is maintained and controlled by a third party. Highly personal information is entrusted to an unknown entity. A physical wallet owner is responsible for protecting his/her identity. With a digital wallet, the owner’s risk profile is different. Consumers may not be fully aware of the protections needed, nor do they anticipate the problems, and incorporate appropriate risk mitigation tools.\(^7\) Do you really know what you are giving up with your digital wallet and the implications for your personhood and individual identity?

How does a mobile digital wallet application work? Using a mobile device, the software application is stored on the physical mobile phone to manage and initiate payments. The owner enables the payment transaction by opening up the application (app) on the mobile phone, and waving or tapping the mobile digital wallet over an NFC-enabled terminal or retail location. Near field communication (NFC) is a standards-based wireless radio communications to exchange data between devices a few centimeters apart (e.g. mobile phone and merchant point of sale).\(^8\) A secure element (SE), which is a tamper resistant encrypted smart chip on the mobile device, stores and manages access to

---

\(^7\) Federal Reserve Bank of Boston, *Mobile Phone Technology: "Smarter" Than We Thought*, November 2012, 27.

the customer account credentials for NFC contactless payments.\textsuperscript{9} This means that sensitive financial information is stored on the mobile device.

A digital wallet can also store the payment information on a secure remote server known as the cloud. The primary difference from the NFC mobile wallet is that sensitive financial information is stored on the cloud and not on the mobile phone. A cloud based or digital wallet stores the financial information remotely from the mobile device, and sends only tokens or authorizations to the actual mobile phone to initiate and authorize the payment at the point of sale (POS). A wireless service, either cellular or Wi-Fi, is needed to complete the digital wallet transaction.\textsuperscript{10}

A hybrid mobile wallet leverages the security aspects of NFC and the added protection of storing the real payment credentials in the cloud. The consumer’s financial information in the cloud is linked to a mobile phone though a unique identifier in the device. Account credentials used when making point of sale (POS) mobile purchases are accessed from the cloud when needed, but the payment transaction is still initiated using the NFC protocol to communicate from the mobile phone to the POS terminal.\textsuperscript{11}

What does your wallet choice say about you as a person? Selecting a physical wallet is a personal choice, for example, the material, color, design. There may be a dimension of value, a brand name with a cachet you associate with, like Louis Vuitton or


\textsuperscript{10}Federal Reserve Bank of Boston, \textit{Mobile Phone Technology: “Smarter” Than We Thought}, November 2012,1-30.

\textsuperscript{11}Ibid.,3.
just a good value, like a discount name brand wallet you stumbled on at Century 21 Department Store.

An independent consumer magazine recently compared the features of four popular digital wallets, including their convenience (i.e., where is can be used), protections, and security.\(^{12}\)

Is a digital wallet more convenient than pulling a credit card out of a physical wallet? Yes, reports the consumer research magazine survey, if you are “standing on the checkout line and have your smart phone out because it is no trouble to open the wallet application, punch in a PIN, and hold the phone over the card reader to pay.” But they report that a digital wallet may not be more convenient than a wallet if you have to pull it out of your pocket and launch the application. Another potential drawback is the battery life of your mobile wallet. A physical wallet may be tattered and old from wear, but it does not run out of battery life and die at the register in the middle of a transaction.\(^{13}\)

Can digital wallets be used anywhere? The consumer research magazine survey explains that certain NFC mobile wallets may not work at all store registers. Where you can use a digital wallet becomes important because you can use your physical wallet anywhere. Typically, merchants take cash, and you also store your credit cards in your


\(^{13}\)Ibid.
physical wallet. A mobile wallet may not be much use if the store you are shopping in does not accept it as a form of payment.\textsuperscript{14}

The consumer research magazine survey notes that some of the same security and privacy concerns associated with a physical wallet are also present for a digital wallet, so losing either can be enormously disruptive. The credit cards in a physical wallet, as well as those loaded on a digital device, are protected by certain federal regulations or voluntary industry protections. Your physical wallet could be stolen, along with your credit cards, license, and other forms of personal identification stored in the wallet. Nefarious individuals could also attempt to access your bank, credit card, or other accounts, irrespective of whether your wallet is in your back pocket, purse, or in the cloud.

Does digital wallet security presents additional security and privacy challenges? Data may be encrypted on the digital wallet, along with requiring a PIN to unlock the wallet, for added protection. But the survey notes that certain digital wallets allow the consumer to disable this feature, exposing the digital wallet owner to potential fraud. Consumers may be more susceptible to their privacy and invasive data collection by retailers, social media concerns, and others that will be explored more fully in a later chapter.

Does a digital wallet offer tighter security than pulling out a credit card from a physical wallet at the checkout counter or online? A typical purchase by credit card involves the consumer providing the merchant with a credit card so the store can obtain

\textsuperscript{14}Ibid.
approval from the credit card provider. The merchant will likely keep this card number on its server, and may become the target of cyber criminals looking to steal credit information.\textsuperscript{15}

Security advancements by certain digital wallet providers are designed to eliminate exposing a consumer’s credit card information to the merchant. A popular digital wallet provider instructs the digital wallet owner to take a picture of their credit card using their smartphone (issued by the digital wallet provider). The digital wallet provider confirms the card with the wallet owner’s bank and then deletes the photo. The credit card number is not stored on the smartphone or by the digital wallet provider. The digital wallet provider creates an encrypted string of data called a device account number that stands in for the credit card and is stored on the phone in a special chip referred to as a secured element (SE). The device account number cannot be accessed by an application on the smartphone other than the digital wallet provider.

The payment is triggered by touching the smartphone which responds only to the owner’s fingerprint. The SE activates the device account number and combines it with data about the transaction to create a unique code for the sale. A payment processor, commonly the credit card issuer, recognizes the device account number and unique code and it uses them to approve or reject the transaction. The merchant never sees the consumer’s credit card.\textsuperscript{16}


\textsuperscript{16} Ibid.
A global consulting firm studied the awareness, usage, benefits, drawbacks, and likelihood of consumers using a mobile digital wallet to make purchases, transfer funds, conduct financial transactions and carry identification such as a driver’s license or medical insurance. Their research explored which types of institutions consumers would trust most and would consider most capable of managing a mobile wallet.\(^\text{17}\)

Their research found that mobile digital wallets let consumers store everything from their credit and loyalty cards to their personal information in one organized, accessible place in their smartphone. Consumers are highly aware of mobile applications offered by the top wallet providers and find the convenience and money-saving incentives appealing. However, many consumers hold back from using mobile wallets because of security and privacy concerns. Consumers worry about their liability if the mobile phone is lost, stolen, compromised, and have significant concern that their smartphone will become a greater target for theft if it evolves into a mobile wallet. Consumers like the idea of using mobile wallets to store easily replaceable items like loyalty and membership cards, coupons, a paperless ticket. They are less comfortable with storing cash on their mobile phones or using them for highly personal items like social security cards or electronic keys to their car or home.\(^\text{18}\)

According to a global research firm’s recommendations, companies should address security concerns and defensive measures to protect mobile wallets, such as fingerprint identification technology. These preventative and restorative measures offer


\(^{18}\) Ibid., 1-13.
consumers peace of mind. They report that consumer want widespread acceptance of
digital wallets in places like gas stations, retailers, and doctor’s offices. When it comes to
managing mobile wallets, their research revealed that consumers place trust in banks and
credit card companies, believing that financial institutions are the most experienced and
trustworthy at handling personal and financial information. Consumers placed less trust
in entities like phone service companies and retailers to manage mobile wallets.19

The global research firm offers companies ideas to connect with the consumer on
the move by easing security fears, offering money saving incentives, and promoting
wider acceptance. But there is no mention of educating and informing consumers about
digital wallets. The primary focus is from the retailer’s perspective, capitalizing on
growing awareness and usage, offering incentives to use mobile wallets through money
saving opportunities, and emphasizing convenience. 20

To achieve broader consumer acceptance, the report recommends that retailers
respect personal space and privacy so that consumers do not feel tracked and bombarded
with recommendations and offers on their mobile digital wallet. Building consumer
confidence in the mobile wallet concept to convey convincing security measures was
advised. Consumers are looking for broader acceptance of digital wallet payments of
seventy-five percent or more by retailers and other institutions too. Making replacement

19 Ibid.
20 Ibid.
digital wallets as painless as possible with a 24-hour replacement guaranty was also considered reassuring.  

Consumer concerns about digital wallet security have contributed to their slower than anticipated growth. When you lose your physical wallet, it is your duty as the account owner is to identify the credit cards, debit cards, and other forms of identification, and contact the respective customer service agents to report the cards as lost or stolen, cancel, and replace the cards. You will likely be covered by existing consumer protection laws.

What happens when a digital wallet is lost or stolen? Digital wallet providers continue to advance their technology around security. Two large digital wallet providers have been cited for advancing security strategies. Provider G protects the digital wallet with a PIN that only the wallet owner knows. Provider A’s wallet is protected using a Touch ID (biometric fingerprint authentication).  

When the digital wallet owner realizes their device is lost or stolen, he/she would then go to Provider G or Provider A’s website and place the device (i.e., phone) in what is referred to as lost mode. If, or when, the phone comes online, it will immediately be placed in lost mode, enabling the security. Assuming a technically savvy fraudster has possession of the phone and circumvents Provider G’s PIN security, the phone is in lost mode and will refuse to make any payment transactions even if the PIN was hacked. In the case of Provider A, the token stored inside the embedded secure element will be

---

21 Ibid., 2.

erased making it impossible for the fraudster to perform a payment transaction even if they hacked the Touch ID.\textsuperscript{23}

Once the digital wallet owner has enabled the lost mode on their provider’s website, there is no need to contact the card issuers loaded on the digital wallet. The digital wallet owner can continue to use the credit cards without having to wait for a new card to be issued.

But lost mode can only be communicated to your digital mobile wallet if the phone is online. If the phone does not come online, Provider G and Provider A are not able to initiate lost mode to their respective mobile wallets. In this case, Provider A assumes that its biometric fingerprint offers enough protection to deter the fraudster. It may still be prudent for the mobile wallet owner to contact the credit card issuers to cancel their cards. Provider G’s PIN may not offer as strong a protection as a biometric fingerprint, potentially leaving a gap. However, Provider G uses a cloud server, so if a payment transaction were to occur, the transaction has to pass through its server and will be rejected by Provider G at the server side.\textsuperscript{24}

Is a digital wallet smarter than a physical wallet because its design provides a better experience? There may be more to what is in our wallets than just objects.

\textsuperscript{23}Ibid.

\textsuperscript{24}Ibid.
CHAPTER 3: ETHICAL AND SOCIAL MALADIES

This chapter explores whether the existence of digital wallets leads to ethical and social maladies through a review of relevant research.

Lanier observes as follows:

What effect technology will have on the distribution of wealth and opportunity in our society is not a new question, of course. It was widely obsessed over in the nineteenth century, as it became clear that industrialization was transforming the world.¹

Digital wallets pose a range of questions around privacy and its relationship with identity and personhood. Identity and data collection through the use of digital wallets and the need for a “right to identity” was explored by Serge Gutwirth in “Beyond Identity.” Like Lanier, he associates the internet’s Web 2.0 design to the increased availability of information generated by users and their social interactions. Gutwirth questions whether this also increases the ability to infringe on a person’s identity through data collection and profiling.²

Gutwirth observes that monitoring systems, not humans, collect and exchange data, developing a profile of a person and their behavior, potentially without their knowledge. Government and private actors then assess an individual’s behavior continuously in order to fit them into new, temporary profiles that those individuals

¹ Lanier, You Are Not a Gadget: A Manifesto, xi.

cannot control and which they are often not even aware of. He questions whether these profiles will be abused, potentially leading to unfair discrimination.3

Is it possible to know whether a digital wallet owner’s profile is being created to determine credit and other characteristics that may categorize or pre-judge them? Is it any different than a credit card company or credit rating agency compiling a person’s credit history using the contents of their physical wallet? Unlike a digital wallet, a physical wallet may not have the same capabilities when it comes to monitoring and tracking consumer spending habits.

The feasibility of an individual exercising informational self-determination in an era of network grid computing, data creation, surveillance and online fraud was considered by Ann Cavoukian in “Privacy in the Clouds.” She also refers to Web 2.0 as the latest stage of an ongoing revolution in information and telecommunications technologies that generates, transmits, and stores data volumes at a rapid growth rate.4

Cavoukian believes that technology has created “de facto digital wallets” under our control that “interact with the network grid and serve as brokers and proxies for our identity based transactions in the digital worlds.” She notes that a user centric approach to managing personal data is problematic because a third party, rather than the user, has control over a person’s personal data. The author argues for a digital management

3 Ibid.,124.

infrastructure to better manage our digital identity that would include laws, standards, educational awareness, and market forces to support her vision.5

A data analytics research firm offers a different perspective on data collection involving digital wallets, while acknowledging the “creepiness factor” associated with targeting and consumer privacy concerns. They advocate that digital wallet technology provides the retailer with contextual information about the consumer’s spending habits, purchase history, and product preferences. The retailer can then make informed purchase recommendations to a consumer using this information along with the consumer’s real-time location. Their research indicates that younger consumers may have fewer concerns about this type of data collection, be more open to digital interaction, and not perceive it as targeting or being profiled.6

Do consumers spend more using a digital wallet because they either perform product research leading to purchase of a complementary or higher priced items, or take advantage of a discount or coupon found online which causes them to buy more overall? Do consumers also spend more because they feel less pain using a digital wallet compared to paying in cash?

The “pain of payment” concept has primarily been associated with credit card usage, and the immediate pain experienced when individuals are purchasing goods or services using cash compared to a credit card. One research group believes that a digital

5 Ibid., 4.
wallet may produce similar effects on spending behavior as a credit card does since the

Behavioral economist Daniel Ariely’s research on the pain of paying divides the total aversion to making a payment into three elements. The first element is the disutility of payment which is described as the opportunity cost in utility of the money that is spent. The second element is the hassle associated with paying, for example clicking a link may be viewed as less hassle than filling in a several lines of information for a credit card. The third element is the remaining aversion to making a payment when the effects of foregone utility and hassle are taken into account. This is referred to as the pain of paying.\footnote{Daniel Ariely and Jose Silva,“Payment Method Design: Psychological and Economic Aspects of Payments Paper 196,“ Center For Business@MIT, August 2002, 4-5, http://ebusiness.mit.edu/research/papers/196_Ariely_PaymentMethods.pdf,(accessed 2015).}

Ariely identifies two general goals of understanding payment methods: examining the psychological aspects involved in payment, and examining the effects of different payment methods on expenditures and consumption. The psychological aspect of the pain of paying plays a large role in the effectiveness of payment methods. While consumers might be aware of some of the effects of payment methods, according to Ariely, they may not be aware of the effects of payment methods on spending and consumption. Whether a
consumer’s intuition is wrong, Ariely explains, reflects the novelty of the different payment methods used or possibly a more deeply rooted bias.⁹

Ariely believes that an important aspect of research is the consumer’s reaction to payment methods where multiple payment methods coexist in the marketplace. Will the effects of such payment methods be as strong when consumers are aware of the different options? Will the consumer use these methods to control their own behavior? Will they chose different payment methods for different types of products? ¹⁰

Ariely looked at the effects of the pain of paying in the context of digital wallets. If a website allows pre-payment into a digital wallet, the consumer views this as a sunk cost. In this case, the consumer may overspend because the apparent cost of consumption to the consumer is zero, despite the fact that there is a real opportunity cost, since the money in the digital wallet account is really fungible and could be used for different purposes.¹¹

Does this suggest that a digital wallet could elicit impulsive behavior, allowing the consumer to make purchases without reflecting on its consequences? Consumers make similar choices using a credit card or a debit card from their physical wallet rather than paying in cash. Some would argue that the motion of pulling out a physical wallet to hunt for a credit card means you are paying for something that causes more pain compared to the swipe of a mobile digital wallet.

---

⁹ Ibid., 26.
¹⁰ Ibid.
¹¹ Ibid.
Consumer shopping behavior using mobile digital wallets has also been surveyed by the Federal Reserve System (Federal Reserve). A 2014 survey administered by an online consumer research firm, on behalf of the Federal Reserve, randomly sampled over 50,000 individuals. The survey noted wide use of mobile phones, with eighty-seven percent of the U.S. adult population owning a mobile phone. Seventy-one percent of mobile phones are smartphones. According to the survey, consumers appear to be open to greater use of their phones to get the best prices in their shopping activity. Of those surveyed, twenty-four percent were interested in using their mobile phones to compare prices while shopping, twenty-six percent would like to receive and manage discount offers and coupons, and twenty-four percent would like to receive location-based offers. There was also a nineteen percent interest in using their phones to store gift cards or track loyalty/reward points. 12

While consumers may be willing to use their phones to improve shopping experiences, many are resistant to sharing their current location and personal information with companies they shop with regularly. Consumers are even less willing to allow smartphones to be used to provide companies with their personal information to receive targeted discounts, promotions, and offers. Smartphone owners were asked about their level of agreement with a statement about their willingness to allow their mobile phone to provide personal information to companies they regularly shop in order to receive

---

targeted discounts, promotions, or services from the merchant. Thirty-seven percent chose to disagree and thirty-nine percent chose to strongly disagree.\textsuperscript{13}

The Federal Reserve reported that consumers use their phones to comparison shop and obtain product information while in retail stores. Among smartphone owners, forty-seven percent said that they have used their mobile phones to comparison shop on the internet while at a retail store, and thirty-three percent have used a barcode scanning application for price comparisons. Consumers also use their smartphones to obtain product information, thirty-one percent have scanned a QR code in a newspaper, magazine or billboard advertisement to obtain information about a product, and forty-two percent have used their phone to get product reviews or product information while shopping at a retail store. Many consumers who use a smartphone to comparison shop reported that they altered their decisions as a result. Sixty-nine percent who have comparison shopped in a store reported that they changed what they purchased as a result of reading a product review on their smartphone while at a retail store.\textsuperscript{14}

The Federal Reserve survey also revealed that mobile phones are prevalent among the unbanked (13\%) and the under banked (14\%). Sixty-seven percent of the unbanked have access to a mobile phone, of which sixty-five percent are smart phones. Ninety percent of the under banked have access to a mobile phone, seventy-three percent of

\textsuperscript{13} Ibid.,23.

\textsuperscript{14} Ibid.,24.
which are smartphones. Forty-eight percent of under banked consumers had used mobile banking in the twelve months prior to the survey.\textsuperscript{15}

The Federal Reserve considers the prevalence of mobile phones, and in particular smartphones, among minorities, low-income individuals, and younger persons, to have the potential to empower consumers and expand access to financial services for the underserved population. But they also believe that consumers will need to understand and weigh the perceived benefits and potential risks to their security and privacy.\textsuperscript{16}

The digital divide describes a gap between those who have ready access to information and communication technology, such as digital wallets, and the skills to make use of the technology, and those who do not have access or skills to use those same technologies within a geographic area, society, or community.

Mobile digital wallet usage is expected to add the most value and potentially bridge the digital divide because of the ability of lower income individuals’ access to mobile phones. Depending on the features of the phone, there may be the potential to improve the inequality issue or income issue particularly if the consumer has better access to such things as loyalty programs and rewards. But the tradeoff may be that the mobile wallet payments are not necessarily more secure.

Are identity and personhood issues overshadowed by the desire to provide a service to the underserved and under banked, particularly in developing or poorer

\textsuperscript{15} Ibid., 2.

\textsuperscript{16} Ibid.,27.
The World Bank (WB), in a series focusing on mobile applications, suggests that mobile money may promote financial inclusion.

WB argues that exclusion from the formal financial system has increasingly been identified as one of the barriers to a world without poverty. The use of only informal instruments means the poor are limited in their ability to save, repay debts, and manage risk responsibly. On a macro level, WB believes that these financial constraints on the poor can slow economic growth and exacerbate inequality.

WB writes that along with extending financial services to the poor, mobile money is expected to improve productivity, increasing the efficiency and lowering the cost of transactions, improving security, generating new employment opportunities, and creating a platform on which other businesses can grow. Challenges still remain in a wider acceptance and usage of mobile digital wallets, including the availability of technology capable of reaching dispersed consumers who may be poor and live in remote locations.17

A Federal Reserve-sponsored working group also supports the goal of financial inclusion to help low and moderate income and underserved consumers enter the financial mainstream. Emerging technologies, such as mobile digital wallets, are viewed as potentially decreasing costs to the underserved population. The working group believes it is important to move the underserved into the banking system for financial management, financial literacy, and security of financial transactions. A key theme raised in the report more broadly is the belief that regulators have an interest in ensuring safety

and soundness and consumer protection in the emerging mobile payment environment.  

As the underserved and unbanked gain more access to digital wallets, the need for more education and consumer protections has been raised.

The Bill and Melinda Gates Foundation, the Better Than Cash Alliance, and The World Bank (WB) reported that the rapid development and extension of digital platforms and digital payments can provide the speed, security, transparency, and cost efficiency needed to increase financial inclusion at the scale required to achieve G-20 goals. The Group of Twenty (also known as the G-20) is an international forum for the governments and central bank governors from 20 major economies. The World Bank is an international financial institution that provides loans to developing countries for capital programs. Studies show that broader access to, and participation in, the financial system can reduce income inequality, boost job creation, accelerate consumption, increase investments in human capital, and directly help poor people manage risk and absorb financial shocks.

In 2010, the G-20 endorsed Principles for Innovative Financial Inclusion to provide guidance for policy and regulatory approaches. Evidence exists that the widespread adoption of digital payments can be instrumental in reaching the goals of the

---


20Ibid., iii.
G-20, including digitization, helps overcome some of the costs and physical barriers that have been perceived as impediments to financial inclusion efforts. Digital platforms are viewed as offering the ability to rapidly scale up access to financial services using mobile digital wallets, and other broadly available access points, when supported by an appropriate financial consumer protection framework.²¹

Digital payments can, according to the study findings, also promote women’s economic empowerment by facilitating greater account ownership and asset accumulation, and increasing women’s economic participation.

In the case of government, while people think of their interaction as being intrusive and collecting data, the WB highlights the benefits especially from the developing world. Digitizing by governments has the potential to dramatically reduce costs, increase efficiency and transparency, help build infrastructure and broaden familiarity with digital payments. When governments shift their social, salary, procurement payments, taxation, and licensing receipts to electronic form, the WB contends this creates a foundation on which the private sector and person-to-person payments can build.²²

Some regulators may be hesitant to embrace digital wallet technology. WB advocates that governments need to encourage regulators to enable digital financial services in order to achieve G-20 goals, and specifically should: foster competition by enabling a broad range of providers to introduce new vectors of financial services,

---

²¹ Ibid.,7.
²² Ibid.,4.
ensure that consumer protection and risk based prudential and integrity requirements are met, address cost of entry, and encourage business model innovation to address critical concerns that confront regulators, including anti-money laundering and terrorist financing.\textsuperscript{23}

WB also recommends convening the public and private sectors together to create a basic payment infrastructure. They believe this could enable competing product development, create an environment that fosters private sector innovation, and guide digital financial service providers to educate consumers and small businesses about their options to increase confidence, competence, and adoption.\textsuperscript{24}

The security, convenience, and other benefits of mobile digital wallets could lead to its widespread adoption for everyday purchases by 2020, according to a non-random sample survey 1,020 technology stakeholders and critics. Sixty-five percent agreed that by 2020 most people will have embraced and fully adopted the use of their mobile digital wallet device swiping for purchases rather than pulling out their physical wallet, eliminating the need for cash or credit cards. But thirty-three percent agreed that people will not trust the use of certain technology and there will not be a major conversion of money to a digital only format.\textsuperscript{25}

\textsuperscript{23} Ibid., 13.

\textsuperscript{24} Ibid., 15.

\textsuperscript{25} Pew Research Center, \textit{The future of money: Smartphone swiping in the mobile age}, April 17, 2012, Aaron Smith, Janna Quitney, and Lee Rainie. This was part of a broader survey of 12,000 experts and members of the interested public to share their opinions on the likely future of the Internet 2,551 responded to at least one of the questions in the survey. http://www.pewinternet.org/files/old-media/Files/Reports/2012/PIP_Future_of_Money.pdf, (accessed 2015).
Some of the top technology experts sampled thought that the movement to digital mobile wallets would be slow due to, among other things, resistance from financial stakeholders in the legacy payment structure, privacy concerns, generational preferences, lack of infrastructure to support widespread adoption, and socio-economic factors.\textsuperscript{26}

Proponents of mobile digital wallet systems sampled responded that mobile digital wallets hold a number of advantages over the use of cash and credit cards for payment. Mobile digital wallets were viewed as simpler and more convenient for consumers as a single all-purpose device. Location and tracking devices of consumer behavior were weighed against the perceived benefits of advanced personal shopper services, improved loyalty programs, and more targeted promotions from vendors among other things. One respondent expected that financial institutions would continue to push the mobile digital wallet forward as a significant proportion of population who are “swayed more by superficial comfort rather than by more subtle concerns such as the concern for privacy.”\textsuperscript{27}

Monopoly of power concerns were raised by one survey respondent who questioned whether transaction processors and financial institutions and other incumbents have a vested interest in the current closed source infrastructure which “enables their continued monopoly and the revenue it generates.”\textsuperscript{28}

\textsuperscript{26}Ibid., 27.

\textsuperscript{27}Ibid., 12.

\textsuperscript{28}Ibid., 13.
A social innovation consultant identified a range of opposition issues from technology identity advocates to liberals who oppose the expansion of corporate social control to social justice activities representing impoverished communities lacking access to mainstream financial institutions.29

Technological developments that give rise to ethical, political, and social implications and the role of engineering were explored by Karl Stephan, senior member of the IEEE Society on Social Implications of Technology (SSIT). SSIT is a society that encourages engineers and allied professionals to be introspective and think about what they are doing, why they are doing it, and the effects their actions will have due to their development of new technologies.30

Stephan observed that as a result of continual data collection, we have become a society of people that voluntarily broadcasts to the world a great deal of information. The combination of data that is collected about us, and is freely shared, forms a picture of an individual’s life that becomes easier to correlate. He believes that near constant monitoring and reporting of our lives will grow as our society becomes increasingly comfortable sharing more details.31

He questions whether engineers and professionals lack accountability for the tangible and intangible costs for their actions. Stephan also identifies the need to consider...

---

29 Ibid., 22.


31 Ibid., 1757.
the social implication of the past, present, and future technologies as more than an academic exercise.  

The social implication of advanced mobile devices on human identity was also raised by Professor Lara Sriivastava. She explores the social and human implications of advances in mobile technology and the increased personalization of a mobile device. Sriivastava writes that mobile phones have created a new sense of identity for various groups of people, and it is essential for operators and manufacturers to consider security parameters for safeguarding peoples’ identity.

The effect of databases in our personal lives, like those used in digital wallets, was considered by Professor Daniel Solove. The problem with databases is not being watched, controlled, inhibited, or even the lack of ownership in our personal information. The problem that Solove sees is one of power, its effects on our relationships with public and private bureaucracy, and the inability to participate meaningfully in the collection and use of our personal information.

Solove believes we must focus on the effects of databases in our daily lives and the way that they are changing how we think, judge, and decide. He argues for requiring meaningful, unambiguous limits on how data can be used. This would include basic

---

32Ibid., 1777.


guarantees to people that their information is being treated with respect, dignity, and they are informed when their information is disclosed, and they have meaningful participation in the use of the information. It means that even when information is provided it is not owned by its corporate collectors for any use they might devise. It also means that personal information cannot be bought and sold like any other commodity. 35

Your digital wallet may be costing you money if it is linked to a credit that offers bonus rewards even though the wallet is free to use. Credit card companies determine whether a purchase qualifies for certain bonus rewards the card offers using merchant category codes (MCC). MCCs are assigned by the four major payment networks depending on the nature of the merchant using a list provided by the Internal Revenue Service. 36

Many digital wallet service providers charge the transaction to their own payment account because their encryption technology adds a degree of security to the digital wallet owner’s transaction. The purchase to the digital wallet user’s credit card statement will list the digital wallet service provider instead of the retailer where the purchase was made.

For illustration, a digital wallet user could be missing out on a credit card that offers a percentage of cash back at a grocery store because the credit card issuer sees the MCC based on the digital wallet provider, not the grocery store.

35Ibid., 1462.

Some digital wallet providers authorize transactions by tokenization to secure the transaction. This removes the digital wallet user’s credit number and replaces it with a random number (i.e., token) that expires after the purchase. The digital wallet provider would reflect the grocery store’s MCC, and the digital wallet owner would be able to earn the bonus awards.

The contents of a physical wallet in a person’s back pocket or purse may define their identity in a different way than a digital wallet. You know what your physical wallet says about yourself. Do you know what your digital wallet says about you, and to whom?
CHAPTER 4: REGULATIONS, STANDARDS, AND ROLES

This chapter addresses laws, regulations, standards, and supervisory authority that apply to digital wallets. It also considers the roles of the various actors involved in digital wallets, including government regulators and agencies, consumers, digital wallet providers, computer professionals, and merchants.

Several regulators, federal agencies, and standard setting organizations play a role in the digital wallet marketplace. This includes the Federal Reserve System (Federal Reserve), Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), National Credit Union Association (NCUA), Federal Trade Commission (FTC), Federal Communication Commission (FCC), Consumer Financial Protection Board (CFPB), NACHA, and various state regulators.

Developers, particularly in the technology community, may fail to realize how much regulation exists and the ways that digital wallets may bump up against a particular regulation or set of regulations. Digital wallet providers may perceive that their solution is beyond the reach of existing laws and regulations, but many times these perceptions are mistaken. Consumers also may not realize the protections they have, or do not have, when their physical wallet is replaced by a digital wallet.

Digital wallets are subject to many existing regulations and consumer protection laws at the federal and state level. Regulators look through the digital wallet framework to the underlying payment mechanism that leverages the existing (legacy) payments infrastructure. Legacy payments systems include accounts held by banks (i.e., financial institutions), credit card networks, and ACH payments. ACH, or Automated Clearing
House payments, are electronic payments that are created when the customer gives an originating institution, corporation, or other customer (originator) authorization to debit directly from the customer's checking or saving account for the purpose of bill payment.¹

The digital wallet acts as a storage device for customers, holding information from multiple accounts. It may possibly act as a service provider to a financial institution. The digital wallet could also be a regulated financial institution because it transmits funds and value.

FDIC deposit insurance may be available to a consumer using a digital wallet depending on the wallet’s funding source and whether certain conditions, referred to as pass-through conditions, are met. The FDIC is an independent agency of the U.S. government that protects the funds that depositors place in banks and savings associations. FDIC insurance covers all deposit accounts at an insured depository institution (IDI), including: checking accounts, savings accounts, money market deposit accounts, and certificates of deposit. FDIC insurance does not cover other financial products and services that banks may offer, such as stocks, bonds, mutual funds, life insurance policies, annuities or securities. The standard insurance amount is $250,000 per depositor, per insured bank, for each account ownership category.² But consumers may not know if their digital wallet meets the pass-through conditions to qualify for FDIC deposit insurance.


Mobile wallets use the legacy payments infrastructure. Mobile wallet purchases made through a mobile application or mobile browser use a mobile device to present the legacy payment method for a transaction. Instead of reaching for a physical wallet and pulling out a credit card or cash, the mobile device is substituted for the physical wallet that holds a credit card, debit card, or cash to make the payment.\(^3\)

The method of payment that is loaded onto the mobile wallet actually conducts the overall transaction. There are generally two types of payment methods on the mobile wallet, pass-through and staged. Legacy payments system rules and laws apply to both in the same way they apply to other types of digital wallets. But the consumer may not be aware they possess a pass-through or staged wallet payment device, compared to reaching into a physical wallet and knowing that you are paying by cash, check, credit card, or debit card.

A pass-through wallet has the same legal requirements that apply to the underlying payment method in the digital wallet. The pass-through wallet uses form factor substitution and retains the character of the original underlying legacy transaction method. For example, if a debit card was used in the mobile wallet transaction, then it is subject to debit card network rules and applicable laws.

A staged wallet involves two separate but related stages. The funding stage is where the wallet operator, acting as a merchant payee, receives funds through an existing payment method (e.g., credit card, debit card, ACH transfer). The payment stage is where

---

the wallet operator distributes funds to the ultimate merchant payee using an existing payment method (e.g., credit, debit, prepaid card ACH transfer, wire transfer, etc.).

The FTC, a U.S. federal agency that administers antitrust and consumer protection legislation, acknowledges that mobile digital wallet users may not recognize that their protections against fraudulent or unauthorized transactions can vary greatly depending on the underlying funding source.

Credit cards provide the strongest level of statutory protection, capping liability for unauthorized use at fifty dollars. If a mobile digital wallet payment is linked to a bank debit card, a consumer’s liability for unauthorized transfer is limited to fifty dollars if reported within two business days, and up to five hundred dollars for charges reported after two business days. If a consumer does not report an unauthorized debit transaction on their bank account within sixty days after their periodic statement is mailed to them, they may face unlimited liability whether or not the charges result from a lost or stolen card or another electronic transfer. Other funding mechanisms do not have the same statutory protections as credit and debit cards.

Consumers may not be aware of the significance when using a mobile digital wallet payment mechanism linked to a pre-funded account or stored value card, including a gift card or general purpose reloadable card, when it comes to protections that FDIC

\footnote{Ibid.,13.}


\footnote{Ibid.,5.}
deposit insurance provides. This payment structure is generally referred to as a pooled or custodial account.\(^7\)

In applying the insurance limit to a pooled/custodial account at an insured depository institution (IDI), the FDIC recognizes the holders of the access mechanism (e.g., prepaid cards) as the owners of the deposit, if the FDIC standard requirements for pass-through insurance coverage have been satisfied. Alternatively, the card distributor or other named account holders will be recognized as the owner for deposit insurance purposes. The FDIC requires that the IDI’s account records disclose the existence of a custodial relationship. The IDI’s records must also disclose the identities of the actual owners of the funds and the amount owned by each owner. If pass through conditions are not met, the $250,000 deposit insurance maximum will apply to the named owner of the account.\(^8\) For example, if the above conditions are not met, the prepaid program manager would be covered for purposes of FDIC deposit insurance, not each individual cardholder or account holder.

Funds held by entities that are not IDIs may be protected to some extent by state money transmitter laws that govern nonbank entities engaged in retail payment services for consumers. These entities are referred to as money service businesses (MSBs).

Consumers with mobile digital wallets may want to pay attention to developments raised by mobile carrier billing, which is the ability to charge payments directly to a mobile phone bill. It may appear that the billing leverages the legacy payment network or

\(^7\) Ibid.,6.

\(^8\) 12 CFR section 330.5.
infrastructure, acting like a typical charge card. However, an increasing number of third parties have entered into agreements with carriers to place charges on mobile phone bills.

There are currently no federal statutory protections governing consumer disputes about fraudulent or unauthorized charges placed on mobile carrier bills like there are for credit cards issued by financial institutions. As with prepaid cards, consumers rely on the terms of their mobile carrier agreements or those companies’ goodwill when these disputes arise. Mobile carrier billing also raises unique challenges with regard to third parties placing fraudulent charges onto consumer’s mobile carrier bills, a practice known as “cramming.” 9

The CFPB, an independent agency of the U.S. government responsible for consumer protection in the financial sector, is examining extending certain legal protections to digital wallets. This would include liability limits, disclosure requirements for fees and expiration dates, error resolution procedures, and authorization standards for recurrent payments. CFPB is also considering extending protection to general purpose reloadable cards (GPR), which are expanding in usage, and are one of the ways that mobile digital wallet payments are funded.10

CFPB acknowledges that statutes protecting consumers from unauthorized credit and debit card transaction exist, however similar federal statutes do not exist with respect to pre-funded accounts, stored value cards (e.g., gift cards, general purpose reloadable cards and pre-paid debit cards), or mobile carrier billing. It is anticipated that CFPB’s

9 Federal Trade Commission Staff Report March 2013, Paper, Plastic...Or Mobile, 8.
10 Ibid., 6.
proceedings may have significant implications for consumers using reloadable payment
cards to fund digital wallet payments.11

FTC noted the relevance of these issues for mobile digital wallet payments,
particularly since students and the under banked are among the greatest users of general
purpose reloadable cards. More than ninety-one percent of under banked consumers have
mobile phones, and mobile service providers have encouraged their customers to use
general purpose cards as a payment method. The mobile payment service may link to a
consumer’s credit card, debit card, bank account or mobile phone account as a payment
source.

FTC noted that some companies are beginning to fill the gaps in statutory
protections by contractually promising consumer protections in the event there is a
dispute about a payment. But, according to the FTC, the protections are voluntary,
inconsistent, and companies that provide them could withdraw or modify them at their
discretion.

FTC believes consumers should understand their rights and protections when
choosing to pay using a mobile wallet, including their rights regarding mobile payment
services, and the type of funding mechanism used. FTC also thinks companies should
develop policies regarding fraudulent and unauthorized charges, and clearly convey these
policies to consumers.12

11 Lydia Parnes, Tracy Shapiro, Elisa Durrette, Sharon Lee, and Matt Staples, “FTC Recommends
Consumer Protections for Mobile Payment Industry,” Intellectual Property & Technology Law Journal 25,

12 Federal Trade Commission Staff Report March 2013, Paper, Plastic...Or Mobile,11.
Another key concern for consumers using digital wallets is whether their sensitive financial information can be stolen or intercepted. FCC cited a recent Federal Reserve Bank study reported that forty-two percent of consumers are concerned about data security. This concern was the most cited reason why consumers have not used mobile payments and mobile wallets. Consumers are also concerned about hackers gaining access to their phone remotely, or someone intercepting payment information or other data. FTC believes that consumers can take practical steps to secure their sensitive financial information when using a digital wallet.

Digital wallets raise privacy concerns because of the potential for private sector companies to collect a large amount of data. CFPB Regulation P addresses privacy of data, disclosure, and sharing of information. But Regulation P only applies to financial institutions engaging in activities that are financial in nature or incidental to such financial activities. Regulation P requires, among other things, that financial institutions provide an annual disclosure of their privacy policy to their customers. It allows the consumer to opt out of the disclosure of nonpublic personal information to a non-affiliated third party if the disclosure is outside of certain specified exceptions. Regulation P limits the reuse and re-disclosure of nonpublic personal information a financial institution receive from a nonaffiliated financial institution. Regulation P also

---

13Ibid.,11.
provides that the financial institution may not disclose customer account numbers to any nonaffiliated third party for marketing purposes.\textsuperscript{14}

Mobile digital wallet operators include new actors, such as operating system manufacturers, hardware manufacturers, mobile phone carriers, application developers, and coupon and loyalty program administrators. Third party providers are able to gather and consolidate personal and purchase data unlike traditional payments regimes (e.g., credit or debit cards). These third parties have access to more detailed data about a consumer and the consumer’s purchasing habits, as compared to data collected when a consumer makes a traditional payment method using a bank, or credit card network.

Does this data consolidation benefit the consumer? Some argue that the consumer benefits because the merchant is able to offer products or services that a consumer is more likely to want by knowing in advance the consumer’s preferences. But whether these new actors that consolidate the data are subject to federal or state oversight to provide consumer protections depends on among other things, the type of entity, nature of activity, and the statutory authority of the regulator.\textsuperscript{15}

FDIC has observed that banks are recognizing the value of customer and transaction data. Banks continue to develop partnerships with nonbank third party providers who may not be knowledgeable about the regulatory environment in which


\textsuperscript{15} Federal Trade Commission Staff Report March 2013, \textit{Paper, Plastic... Or Mobile?}, 11.
financial institutions operate. FDIC believes that bank oversight of the third party relationship will become increasingly important.\textsuperscript{16}

Third party relationships are subject to oversight under the Bank Services Company Act (BSCA). The BSCA provides federal banking agencies with the authority to examine and regulate activities, functions, and operations performed by third party service providers to the same extent as if these were performed by the financial institution itself. Bank regulators are able to initiate enforcement actions against both a bank and its service provider for violations of any law, which frequently includes Section 5 of the Federal Trade Commission Act addressing unfair or deceptive acts or practices. The CFPB’s authority to examine banks and nonbanks subject to its jurisdiction extends to the service provider under authority derived from Title X of the Dodd Frank Wall Street Reform and Consumer Protection Act.\textsuperscript{17}

A trade group representing banks has questioned whether regulatory and supervisory gaps exist in the payment framework with the growth of digital wallets. Alternative payment providers (APPs) may engage in functionally similar activities to that of a financial institution that offers a digital wallet. The trade group argues that new payment products generally require the collection and transfer of financial account and other sensitive personal information, but the legal and regulatory frameworks designed to ensure the privacy and security of such information have not been revised to cover APPs


\textsuperscript{17}12 USC 1867(c).
activities adequately. The trade group believes this regulatory failure has consequences for customers, particularly in the areas of data security and privacy lapses.\(^\text{18}\)

Consumers may believe their digital wallet transaction is protected under Regulation E. However, the trade group notes that when Regulation E does not apply to certain transactions, some banks feel compelled to waive the five hundred dollar liability allowed because of their regulator’s expectations. They compare this to transactions involving APPs who may choose to provide liability protection only consistent with Regulation E requirements, and who are not subject to bank supervisory oversight and their regulator’s expectations.\(^\text{19}\)

An academic legal journal raised similar concerns about Regulation E coverage. They note the lack of consumer awareness that a digital wallet provider may be an alternative payment provider, not a bank, and their digital wallet purchase may not be covered under Regulation E. They also discuss whether a digital wallet owner using an alternative payment provider could face unlimited liability for losses as a result of unauthorized electronic fund transfers from their alternative payment service account.\(^\text{20}\)

The trade group highlights that banks are subject to extensive regulatory supervisory and enforcement scrutiny by their prudential regulators with respect to


\(^{19}\)Ibid., 5.

privacy and data security. However, APPs provide products and services on the existing payment systems, capitalize on innovation in communications platforms, and avoid the reach of traditional financial regulators. The trade group notes that banks and nonbank APPs are subject to data security requirements established in the Gramm-Leach-Bliley Act (GLBA). But the trade group points out the differences in the two sets regulations and regulatory guidance, with banks subject to more demanding standards issued by federal financial regulatory agencies, and APPs subject to the more flexible regulations promulgated by the FTC.\textsuperscript{21}

The trade group notes that APPs face lower odds of facing enforcement actions and sanctions for violations because they are not subject to regular examinations, enforcement actions, and other oversight by prudential regulators. The consequences of punishment for lax data standards, if there were to be a data breach that is discovered by the government, would be less significant than that of a bank. While both banks and APPs may be subject to injunctive relief for violations of the GLBA requirements, only banks face a realistic possibility of civil money penalties. The result, according to the trade group, is different consequences for banks and nonbanks for violations of the same statute.\textsuperscript{22}

The trade group contends that neither state laws nor self-regulatory standards make up for the gaps in substantive standards between banks and APPs. While some federal and state regulators have taken steps to strengthen data security requirements for


\textsuperscript{22}Ibid.,16.
APPs, the trade group contends that actions are limited, preliminary, and additional work is needed to narrow the gap.\textsuperscript{23}

The trade group argues that the uneven data security playing field between banks and APPs has the potential for consumer harm, and places an uneven compliance burden on financial institutions. They also believe banks will bear the brunt of costs in the event of a data security compromise of an APP. This may result in fraudulent charges to the consumer’s account. Even when APPs are in theory responsible for directly reimbursing consumers for unauthorized transactions that occur on their platform, when APP accounts themselves are compromised customers are likely to turn to their banks that might be more responsive to customer inquiries.\textsuperscript{24}

Wyndham Hotels & Resorts LLC’s appeal of a recent FTC complaint against the hotel chain for alleged lax tax data protection practices is being watched closely by banking officials who say it could lead to uncertainty over cybersecurity regulations for emerging technologies, including mobile wallets and digital payments. In the absence of a national data standard, the ruling could leave some APP and mobile payment providers not covered by the Gramm-Leach-Bliley Act (GLBA) cybersecurity requirements uncertain of which practices could run them afoul of the FTC.\textsuperscript{25}

The case may lead to uncertainty for banks and other financial institutions if Congress applies a proposed national data security standard to banks. Banks would be

\textsuperscript{23}Ibid., 17.

\textsuperscript{24}Ibid., 2.

exempted from any new national standard because they are subject to GLBA data security and notification requirements. But retailers are pushing for the removal of the exemption potentially making them subject to a national standard that would be enforced by the FTC.²⁶

Standard setting groups are playing a role in creating a level playing field for the digital wallet industry. Companies join standards setting groups to represent their interest and build momentum. One such group is the Mobile Payments Industry Workgroup (MPIW). It was convened in January 2010 by the Federal Reserve Banks of Boston and Atlanta through their Payment Strategies and Retail Payments Risk Forum groups, and is composed of private and public sector participants. The MPIW facilitates discussions among key stakeholders as to how a successful mobile payments system could evolve in the U.S. It meets routinely to share information and ideas, discuss barriers and opportunities in mobile payments and suggest a vision for the building blocks an effective and secure mobile payment system. While it may seem counterintuitive to bring competitors together to collaborate on technology, the Federal Reserve believes that companies can recognize common problems and reach consensus on interoperable solutions.²⁷

Three key trends have emerged from the MPIW: the need to accommodate the convergence of payment channels (mobile, physical and ecommerce); a strong desire

²⁶Ibid.

among industry stakeholders to provide convenience and value in the mobile digital payment experience through value added features beyond payment that will drive adoption by leveraging coupons, loyalty, and rewards; and the need to reduce payment fraud by removing sensitive payment credential accounts numbers from payment transaction flow.28

The Federal Reserve’s report recognizes the role standards organizations play in creating a level playing field in the mobile wallet industry, particularly in a rapidly changing technology environment where regulations may not be able to keep pace with changing technology. Standards organizations, through its members, are viewed as fulfilling a distinct need in the market by evaluating business requirements for various technologies. Standards organizations are seen by the Federal Reserve’s report as consensus builders and collaborators among industry stakeholders. But this can be challenging because there is a range of stakeholders. Mobile payment vendors and other providers come from diverse backgrounds ranging from financial services to telecom and IT solutions. Success, notes the Federal Reserve’s report, requires traditional payment system and mobile industry nonbank cooperation and collaboration for standards, security requirements, customer service and support, and use of consumer data.29

The Federal Reserve also writes that standards organizations may be able to produce requirements or technical specifications for digital wallets that provide industry

28 Ibid.,28.

29 Ibid.,13.
stakeholders with a baseline for developing their own customized solutions, reduce complexity, and support interoperability.\textsuperscript{30}

A key stakeholder in digital wallets is The Electronic Payment Association, also referred to as NACHA. It is a nonprofit association, representing more than 10,000 financial institutions to foster dialogue and strengthen ACH payments. NACHA facilitates and administers private-sector operating rules for ACH payments. Certain digital wallet payments use the ACH network. NACHA issues bulletins to help categorize the roles of parties in digital wallet payment scenarios involving the different types of third party payment intermediaries, as well as clarify how ACH transactions should be identified for consumers.\textsuperscript{31}

Mobile payment adoption is challenged by the convergence of issues beyond what a digital wallet is, or regulations and standards, according to another Federal Reserve study. Consumers are confused by competing technologies that impact merchant decisions, the emergence of nonbanks and disintermediation, and a fragmented market place. The Federal Reserve believes this contributes to issues of data security and privacy, lack of standards and interoperability, and a complex regulatory structure.\textsuperscript{32}

\textsuperscript{30}Ibid., 13.


Digital financial inclusion, including the use of mobile digital wallets, is considered to be a game changer remarked Bank for International Settlement (BIS) General Manager at the 2nd Annual Global Partnership for Financial Inclusion Conference on Standard-Setting Bodies and Financial Inclusion. BIS is an international company owned by central banks to "fosters international monetary and financial cooperation and serves as a bank for central banks."33

Digital financial services, including digital wallets, are considered to have the ability to offer financial services for millions of financially excluded, underserved, and poor populations. BIS reported that banks and nonbanks are improving access channels for those already serviced by banks and other financial institutions. Innovative digital financial services involving the use of mobile phones have been launched in more than eighty countries, resulting in significant advances in the accessibility and affordability provided by digital financial services.34

The benefits of expansive digital financial inclusion are believed to include economic growth and stability for customers and economies. But the policy brief notes that use of these services by formerly excluded or underserved consumers also brings risks because of the characteristics of a typically poor consumer who may be inexperienced and unfamiliar with consumer rights.35


34 Ibid.,1.

35 Ibid.
The policy brief was intended to provide national and global policy makers with a picture of the rapid development of digital financial services for the poor and the need for their attention and informed understanding. The brief defines digital financial inclusion, summarizes its impact on financially excluded and underserved populations, and outlines the new and shifting risks of digital financial inclusion models that are significant to regulators, supervisors, and standard setting bodies (SSBs). It concludes with observations on digital financial inclusion issues on the policy-making horizon.

The policy brief notes that some policy makers are leaning toward product standards and guidelines to complement digital innovations in disclosure and recourse. In the event the consumer suffers a loss, liability can be unclear due to multiple parties involved in service delivery, both agents and third-party providers in communications and technology services. The policy brief identifies the need for significant coordination and communication among regulators and supervisors at the country level as well as the global level for SSBs and other international bodies. Meaningful and manageable privacy principles at the national and global levels to protect against fraud and privacy intrusion were also recommended. 36

As policymakers consider the benefits of providing consistent protections for digital wallets against the costs of implementation, consumers may want to consider the motivation behind replacing a plastic card in their physical wallet with a digital wallet. Consumers may perceive that pulling out their physical wallet and paying by cash and

---

36Ibid.,3.
credit cards is easier, provides more protections, and is more secure, than paying with a digital wallet.
CHAPTER 5: PARADIGM SHIFT?

In this chapter, I analyzed whether the introduction of the digital wallet represents a paradigm shift.

Paradigm is a model or pattern for something that may be copied; a theory or group of ideas about how something should be done, made, or thought about. Paradigm shift, a concept introduced by American physicist Thomas Kuhn, is an important change that happens when the usual way of thinking or doing something is replaced by a new and different way. Would the transition from cash to credit cards to digital wallets be considered a paradigm shift?

A digital wallet is a software application that runs on a smartphone and stores payment information. A consumer moves the smartphone close to the merchant’s receiver and the payment is made, similar to the consumer swiping a debit card or credit card to make a purchase. But is this a paradigm shift?

There is no conclusive support for a paradigm shift at this time. Digital wallets use existing payment platforms. To pay for a purchase using a digital wallet, a consumer still needs a bank account or a credit card.

Instead, would it be more accurate to characterize the introduction of digital wallets as a disruptive innovation as defined by Clayton Christensen? Disruptive innovation is a process or service that takes root initially in simple applications at the bottom of a market and takes hold, moves up the market, and eventually displaces established competitors. Christensen explains that, as incumbents focus on improving their products and services for their most demanding (and usually most profitable)
customers, they exceed the needs of some segments while ignoring the needs of others. Entrants that prove disruptive begin by successfully targeting overlooked segments and gaining a foothold by delivering more suitable functionality, at a lower price. Incumbents focus on pursuing higher profitability in more demanding segments rather than responding to the new entrants. The new entrants gain market share by delivering the performance that incumbents’ mainstream customers require, while preserving the advantages that drove their early success. When mainstream customers start adopting the new entrants’ offerings in volume, disruption has occurred.1

Why does disruptive theory matter? Christensen believes that applying the theory correctly is essential to realizing its benefits. Christensen uses the example that the first minicomputers were disruptive by virtue of the path they followed from the fringe to the mainstream, not because they were considered superior to mainframes. Christiansen explains that most innovation begins as small scale experiment where a disrupter tends to focus on getting the business model rather than merely the product right. When the disrupter’s product or service succeeds and moves to the mainstream, the incumbent’s market share, and then profitability, begins to erode. The disrupters’ business model is often very different from those of an incumbent.2

The smartphone is an example of an innovative business model used to effect disruption. A smartphone performs many of the functions of a computer. A smartphone

---


2 Ibid., 48.
has a touchscreen that interfaces with the internet, and accesses an operating system capable of running and downloading apps, including digital wallet apps. Christensen explains that the smartphone created a new market for internet access, and eventually challenged laptops as a mainstream user’s device of choice for going online.³

The first consolidated taxonomy framework for disruptive innovation in financial services was developed by the World Economic Forum (WEF), a non-profit Geneva-based foundation, in collaboration with a global consulting firm. The framework explores the transformative potential of new entrants, and innovations on business models in financial services, and how they are reshaping the way financial services are structured, provisioned, and consumed.⁴

WEF’s framework includes six core financial services functions surrounded by eleven clusters of innovation. The two relevant core functions for purposes of this thesis are payments and the cashless world, surrounded by the innovative clusters of mobile payments (i.e., mobile wallets), streamlined payments, integrated billing, and next generation security.

WEF notes that most payment innovations do not disrupt the existing payment processors, but instead modify front end processes to improve the customer and merchant experience. WEF believes the future of payments will see innovations, such as mobile wallets, reduce the use of cash and make payments less visible to payers. Mobile wallets

³Ibid., 48.

will also enable financial institutions and merchants to use data driven customer engagement platforms. According to WEF, as more payment solutions allow customers to link their bank accounts for direct payment and point of sale vendor financing, the use of credit cards could be displaced by these platforms.⁵

The success of any innovative payment solution, as WEF reports, will require a strong customer rationale to switch, as most customers do not consider the existing payment system to be broken. In an increasingly cashless future, WEF envisions that payment providers who can embrace emerging payment innovations to offer differentiated, value added digital experiences, will be able to deepen their relationships with customers, and take a dominant place in the changing financial market landscape.⁶

WEF observes that payment innovations have emerged in the last five years leveraging mobile technology and connectivity to make payments simpler and faster. Common characteristics of successful payment innovations include simplicity (e.g., customers make payments with a single tap on their mobile wallet or automatically by leveraging connectivity), interoperability (e.g., allowing customers to manage and use a variety of credit cards, debit cards or bank accounts for payments rather than a single payment), and value added services (e.g., enabling merchants and financial institutions to interact more closely with customers and deliver additional value such as loyalty cards, promotional offers, etc.). WEF forecasts that the cost of making electronic transactions

---

⁵Ibid.,31.

⁶Ibid., 28.
will fall as electronic payments continue to gain more volume. Reduced costs may also be realized because payment innovation solutions are built on the existing infrastructure.

According to the WEF report, cash will continue to be displaced by electronic transactions as payments innovations make it beneficial for customers to use payment cards even for small denomination transactions. As more transactions become virtual and automated, more payment processes will become invisible to end customers, potentially changing their needs and behaviors. WEF envisions payments and mobility becoming more integrated, and the importance of payment transactions as a potential customer interaction point will increase for merchants and financial institutions.

WEF reported that with greater adoption of electronic payments, more data will be accumulated from payment transactions allowing financial institutions, service providers, and merchants to gain greater understanding of customers and businesses. WEF believes this will lead to greater access to loans as financial institutions gain visibility into individuals’ and businesses’ cash flow and spending patterns, improving their ability to extend loans to customers previously less understood. Payment innovations also pose challenges. WEF writes that outdated identity management protocols are creating risks and inefficiencies, and the need to look at innovative regulatory models and a blueprint for digital identity.

---

7 Ibid., 30.
8 Ibid., 32.
9 Ibid.
A global consulting firm identified four potential disruptions they think will reshape the global payments landscape; two relate to digital wallets. They believe that nonbank digital wallet entrants, including large established technology firms as well as startups, will transform the customer experience, reshape the payments and broader financial services landscape, and pose increased competition for banks. Startups have not been a major threat to the banking industry in the past, but the consulting firm believes that could be different now due to the nature of the new entrants, the prominence of the smartphones as a payment channel, and rapidly evolving customer expectations. To remain relevant, the global consulting firm thinks that banks will need to respond to these changes with new strategies, capabilities, and operating models. The changes as viewed by the global consulting firm include how value is perceived, and data is collected, from customers. According to the consulting firm, individuals may need to balance how they use technology and reap its benefits, with the knowledge that they may give something up as a result.\textsuperscript{10}

The consulting firm envisions the digital revolution extending beyond consumer payments and retail banking, causing significant changes in transaction banking. Customers want faster and more convenient payments for retail purchases, and will soon demand similar conveniences and service levels in transaction banking. The consulting firm forecasts that transaction bankers are becoming more aware of nonbank threats and of the potential major down side of failing to invest in digital infrastructures and services.

The consulting firm thinks the digital banking revolution that started in retail payments is making its presence felt in transaction banking as companies begin to demand convenient and secure services equivalent to that found in the retail sector. They predict that the combined impact of these disruptive forces will reshape the payments industry in the next five years. The consulting firm sees disruption also bringing opportunity for success to those who keep pace with technological change, customer expectations, and the quest for innovative payment solutions.\textsuperscript{11}

A global investment banking firm characterizes mobile payments and the use of digital wallets as revolutionary. Their long term prediction is that combining smartphones with the ability to pay, the fundamental basis of the mobile wallet, will lead to structural business changes fundamentally reshaping entire economies and industries. Consumers will benefit from improved ease of use and security for those currently carrying wallets overflowing with paper and credit cards. They believe this represents the latest evolution and expansion of the global marketplace, with the potential to reach locations that do not have branches, or ATMs distributing cash, and where credit and debit cards are not accepted by cellphone. According to their research, there are 1.3 billion active debit and credit card accounts purchaser compared to nearly 7.3 billion active mobile phone accounts.\textsuperscript{12}

Whether mobile wallets disrupt or amplify the marketplace for financial transaction depends on the market. The global investment firm writes that the current

\textsuperscript{11} Ibid.,26.

electronic payment structure has been in place for nearly half a century and may face some disruption as new digital wallet technology providers emerge. The example they cite is cloud-based digital card payment and wallet solutions. They are already established, but may face disruption as hardware-based options, which allow users to make seamless and secure payments with their mobile devices, are on the rise.\(^{13}\)

Mobile wallets’ success may depend on whether the digital wallet payment system for consumers and retailers is widely accepted, makes transactions easier, and includes robust consumer protections and security. It may also depend on whether mobile wallets can target and drive sales at a low costs for merchants.\(^{14}\)

Another large market place shift is mobile wallets’ ability to offer a big data opportunity on consumer behavior and unprecedented direct access to shoppers. Big data is generally described as extremely large data sets that may be analyzed computationally to reveal patterns, trends, and associations, especially relating to human behavior and interactions. Retailers, marketing firms, analytics companies, and others that aggregate and analyze data may be among the potential beneficiaries of the big data opportunity provided by mobile wallets.

As the investment firm observes, based on specific consumer behavior, GPS, and other data points, retailers can reach out directly to potential customers who use mobile wallets to target offers including rewards, coupons, and loyalty programs. Mobile wallets enable the consumer to then act on the offers using their device. But the investment firm

\(^{13}\) Ibid., 3.

\(^{14}\) Ibid., 4.
argues that this is not impulse buying. Rather, mobile digital wallets may offer consumers transparency and the ability to take control over their finances and budgeting. Instead of acting on an offer when passing a store, the mobile wallet provides the consumer with the ability to check the status of their credit balance, and make an informed decision. Taking it a step further, they believe that parents could receive detailed updates on what and where their children are spending mobile allowances.  

The largest growth opportunities, according to the investment banking firm, are expected in emerging markets. Traditional forms of cash and credit have been challenged in these markets by payment infrastructures that are costly to build, run, and maintain. They believe that digital wallets have the ability to financially empower people in emerging markets by turning anyone into a small business owner because customers can use their mobile phones to pay for goods and services.

A national daily newspaper also writes about the digital wallet revolution. They believe what is revolutionary is the digital wallet’s ability to facilitate a “parallel emergence of virtual purchasing power.” This is described as the digital wallet’s ability to store different types of values, find the best deal, and execute it, ignoring the historical and cultural differences between dollars, points, coins, and virtual property. They believe there will be a shift in thinking about the value of currency based on what the consumer can buy with it, not because the government says it is worth something, or has value.

---

15 Ibid., 5.
16 Ibid., 6.
17 Edward Castronova and Joshua A.T. Fairfield, “The Digital Wallet
Another consumer research firm predicted that massive disruption in mobile wallets would emerge slowly. While digital wallets are accessible through various devices, they expect smartphones to dominate because of their ability to bridge the offline and online world. The future, as the consumer research firm sees it, extends beyond payments as new entrants address consumers’ latent needs and offering more than just more efficient payments. Consumers want a better shopping experience and already use their smartphones in store to compare prices, research product information and reviews, and access shopping lists. The consumer research firm contends that digital wallet providers will continue to investigate marketing opportunities beyond the payment itself.18

Digital wallets have also been viewed as a transformational innovation offering the potential for easier and cheaper access to finance. The perceived benefits include opportunities for revenue growth in existing and new markets, reduced costs of handling cash, efficiencies in managing invoices, receipts, and reducing audit costs. According to editors of a management journal, digital wallets may also create uncertainty and complexity raising doubt over technological choices and lower entry costs, inviting new business entrants to disrupt the status quo.19

---


The authors discuss whether innovations in digital wallets provide societal benefits by reducing tax avoidance, aiding social payments, reducing the health risk of handling germ carrying cash, and conceivably bringing disenfranchised people into the global financial system. Digital wallets may also raise challenging questions of balancing freedoms and openness with the need for oversight and regulation. The authors note the risks and concerns around cyber security and electronic crime, and the need for an appropriate regulatory balance to encouraging private initiatives while protecting citizens.20

The authors believe that using the digital infrastructure provides opportunities for inclusive innovation. Unlike the business models of large corporations addressing the bottom of the pyramid, they suggest that inclusive innovation allows poor people and societies facing problems to develop their own solutions. By using the digital wallet infrastructure, they believe that bottom up ideas can emerge from local entrepreneurship.21

Throughout history, consumers have been skeptical about shifts in payment systems, from the checkbook to the credit card, as one academic online publication notes. Paranoia sets in, but the benefits of the new system emerge and become compelling, consumer protections are put in place, and people begin to adapt to the changes. Credit cards, for example, gained in popularity but not overnight. Consumer trust was built after protections were put in place to limit consumer liability for fraudulent charges up to fifty

20Ibid., 326.

21Ibid., 328.
dollars. They believe similar approaches applied to digital wallets may also increase their popularity. The issue in the U.S. with digital wallets is that most consumers are not convinced they need them. They write that shoppers do not see digital wallets as solving any big problem, and a digital wallet would have to have a clearly demonstrable advantage before consumers gravitate to it.22

The academic online publication also points out that the value proposition in the U.S. is hampered by the hassle and trust factors. Consumers perceive that it is a hassle to link their bank account to the digital wallet along with loading their credit, debit, and loyalty cards. Consumers may also be reluctant to trust a nonfinancial start-up company to handle their financial transactions. Recent studies noted indicate that consumers trust their primary financial institution more than a mobile operator.23

The authors believe that digital wallets will continue to co-exist with physical credit cards for a long while. When shoppers realize the speed and ease with which they can go through the checkout line, they will start to prefer the digital wallet. Finally, the authors note that the digital wallet operator’s technology may not be innovative, but the digital wallet measures something of more value than a single credit card payment, it measures actual purchase behavior which allows for customer targeting, custom pricing, product recommendations, and other strategies.24


23Ibid.,4.

24Ibid.,4-5.
A global technology consulting firm raised a similar perspective about consumers expecting more from using digital wallets than solely the payment mechanism. They believe consumers are looking for a solution that combines payments and a range of services together. At the same time, retailers want to be able to act on what happens before, during, and after the transaction to raise their customer conversion and retention rates by pushing promotion promotional offers through the digital wallet.²⁵

The technology consulting firm contends that if the digital wallet is merely a form of payment acceptance, it may be no more attractive than any other type of payment mechanism.

The technology consulting firm argues as follows:

But the fact is that there are real convergence points between the interests of the consumer and the retailer when it comes to the added value provided by digital wallets. That’s where we’re likely to see solutions emerge. And the promise of seeing these wallets simplify the processes of small and medium-sized firms, or combining into a single product a diverse range of services which today are being provided by various different players, is on everyone’s mind. However, there are as yet no real initiatives underway capable of creating an ecosystem of connected services which do add value for both parties in this way.²⁶

The author of an advanced payment report writes that, at one time, online banking and payments were considered novel, but are now viewed as necessities. Their acceptance was attributed to familiarity, trust, convenience, and consistency of service rather than novel payment features. The payment report notes that consumers are slow to migrate from an existing trusted channel to something new that they have to learn. They


²⁶Ibid.,3.
believe that the success of digital services has to do with how customer needs are met in a convenient, simple and secure manner. Consumers have more choices, and they believe that having multiple regulators in several markets makes it easier for new entities to enter the payments industry to make it more competitive and innovative.\(^{27}\)

An essential success factor for digital wallets is to ensure the entire purchasing process is designed for ease of use. According to the payment report, if consumers have a difficult experience loading a payment card on a digital wallet and perceive it to be cumbersome to enter long card numbers and personal details onto a small mobile phone, or the customer has to wait in line an overall poor consumer experience, this will guarantee the demise of the digital service.\(^{28}\)

Similar to other reports, the most valuable element of a digital wallet is not the payment feature. The value to the consumer is storing the contents of the physical wallet on the digital wallet. An example of how value is added is the ability to add coupons by location-based services. For example, can you digitally load your boarding pass while travelling, your store’s loyalty card, and is the experience balanced with security and being protected against fraud.\(^{29}\)

A recent consumer research poll noted that digital wallet providers will need to convince consumers to adopt and use their product. To achieve this, the consumer poll


\(^{28}\) Ibid., 9-10.

\(^{29}\) Ibid.
suggests that digital wallet providers need to make significant investments in their technology and advertising efforts. They believe a crucial factor in attracting and retaining customers is engagement in order to realize a substantial return on investment.\textsuperscript{30}

The consumer research poll identifies three types of customers. Fully engaged customers are emotionally attached and rationally loyal. They go out of their way to locate a favored product or service and will not accept substitutes. True brand ambassadors are the company’s most valuable and profitable customer. Indifferent customers are emotionally and rationally neutral a take it or leave it attitude. The actively disengaged are emotionally detached customers from a company and its products or services. They easily switch brands and are agnostic to a company. The consumer research poll believes that fully engaged customers will use digital wallets every time, or almost every time, in the past thirty days compared to twelve percent indifferent customers and only two percent of actively disengaged customers.\textsuperscript{31}

While mobile wallet demand is reportedly slow, consumer research firms continue to monitor millennial generation preferences. This generation now outnumbers the baby boomers, and is considered to have the most growth potential. While mobile payment usage is still low generally, younger demographics (18-34 years old) were considered twice as likely to already be using mobile wallets compared to the 35 year old and plus demographics, and more likely to start using mobile wallets for payment in the


\textsuperscript{31}Ibid.
next twelve months. The millennial generation was also more likely to consider using nontraditional payment providers for digital wallet services over established traditional banking institutions. But one survey indicates that the millennial generation has little faith in the security of the digital economy, including digital wallet services.

The evolution of electronic wallets, and their role in enabling a human being to become globally present in the form of a virtual person, was explored in a white paper (White Paper) by a private sector authentication and payment solution company.

The White Paper contends that as humans evolve towards a continuous state of connectedness through the use of information technologies, they will begin to use electronic representations of their familiar items of value. To meet the needs of the digital world, electronic wallets will begin to co-exist with physical wallets.

The White Paper perceives the future of electronic wallets as evolutionary with a need to address the issues of identification and exchange of value over the internet in an easy and reliable fashion. For electronic wallets to become universal, they would need to retain the functionality and usefulness of physical wallets, along with new functionality by taking advantage of the internet medium.

---


35 Ibid., 5.
The challenge, according to the White Paper, is taking all that human beings are accustomed to with them to the digital world. That includes taking the method of exchanging value and the “recognition of their identity” and freeing yourself from physical boundaries.36

The White Paper foresees the future of electronic wallets as a personalized portal for each individual in an emerging electronic world. They write that the rise of ecommerce would force us to invent new payment mechanisms again. Without payments there is no business, and ecommerce cannot exist without an effective means of exchanging value. The author’s conclusion is that the electronic wallet is destined to become the virtual representation of a person on the internet, becoming the owner’s “authorized agent for eCommerce transactions.” 37

Does everyone want their digital wallet be a virtual representative of themselves? If your identity is in your digital wallet, have you lost your personhood? What happens if you lose your digital wallet, do you lose your ability to pay or your personhood too?

36 Ibid., 5.
37 Ibid., 12.
CONCLUSION

Have you thought about what is in your digital wallet? Does it represent your personhood, or a virtual person, and do you care?

This thesis took a closer look at whether digital wallets are determining our identity and deemphasizing personhood, leading to ethical and social maladies.

The ethical malady of privacy assessed digital wallets and their relationship with freedom and autonomy across generations. Digital wallets and data collection were compared to physical wallets. The digital divide as an ethical malady examined the potential gap between those who have ready access to digital wallets compared to those who do not. Digital wallets’ impact on class systems contemplated the potential to raise economic and social inequalities between groups of people. Regulations and standards applicable to digital wallets were studied. Applying the concept of paradigm shift to digital wallets was also considered.

Is there an economic advantage to using a digital wallet over a physical wallet or credit card? The price for technology and the disadvantages for choosing not to use a digital wallet may not be significant. Digital wallet providers use the existing payment infrastructure including credit card networks and ACH payments through a financial institution.

Digital wallets do not appear to include a digital divide as with internet access and banking. Studies indicate the appeal for the under banked and unbanked consumer is reduced transaction costs and increased accessibility. Digital mobile wallets also appear to be favored by lower income and minorities.
Is there evidence of a paradigm shift in payment mechanisms from cash to credit cards to digital wallets? Digital wallets use the same electronic payment structure that has been in place for nearly half a century. To pay for a purchase using a digital wallet, a consumer still needs a bank account or a credit card.

Consumers may perceive that pulling out a physical wallet and paying by cash, debit card, or credit card is easier and provides more protections than paying by a digital wallet. The hassle factor is also associated with a digital wallet because consumers still have to load their credit card, bank, and other information on to the digital wallet.

As policy makers consider the benefits of providing consistent protection across digital wallets against the costs of implementation, consumers may want to consider the motivation behind replacing a plastic card in their physical wallet with a digital wallet.

How a digital wallet works and its interactions with the digital wallet owner may help inform one’s thinking about the impact of the digital wallet on personhood. Unlike a physical wallet, a digital wallet owner may have the perception of autonomy over their wallet, but it is maintained and controlled by a third party. Digital wallet owners may also be more susceptible to privacy and invasive data collection. But security and privacy are a concern for physical and digital wallets.

Using a digital wallet instead of a physical wallet is an individual choice. You are not being forced to use a digital wallet. You control the destiny of your personhood, those qualities that confer your distinct individuality. Do you want your identity in your back pocket or flying around on a cloud or on the internet? Does your physical wallet hold those scraps of paper and to-do lists to remind you to do things that a digital wallet
cannot? Does it remind you to spend less, choose the best credit card to maximize loyalty points, or hold the picture of your loved ones? Your identity is tangible, is your digital wallet? Computer ethics pioneer Norbert Wiener writes as follows:

For human beings to flourish they must be free to engage in creative and flexible actions and thereby maximize their full potential as intelligent, decision-making beings in charge of their own lives. This is the purpose of human life.¹

This is important because people flourish not technology.

After all this research, I informally queried a few millennial generation acquaintances (i.e., 20- something, college-educated, employed, and social media savvy). Some respondents were ambivalent towards the digital wallet value proposition, as well as its imposition on personhood and identity.

The respondents tend to have one credit card and a debit card, are not loyal to any one store, do not appear to be as concerned about having their data shared and tracked by retailers, do not care about the ability to load several credit cards or loyalty cards to a digital wallet (because they do not own multiple cards), dislike carrying a lot of stuff, shop on line rather than go to the mall, and tend to lose either their phone or physical wallet fairly frequently.

Is the physical wallet destined to be replaced by a digital wallet? There is a place for both to co-exist. I do not expect the National Museum of History to feature an exhibit about physical wallets, how they were used, and their ultimate demise, anytime soon.

THE END.

¹Stanford Encyclopedia of Philosophy,5.
BIBLIOGRAPHY


L’Atelier BNP Paribas Group. *Mobile Payments: Surge in digital wallet adoption*


Wheatley, Malcolm.“A Potential Feast for Customer Analytics: Digital Wallets Face


