Financial Consumer Agency of Canada
Agence de la consommation en matière financière du Canada

International Review: Mobile Payments and Consumer Protection

Charles Gibney, Steve Trites, Nicole Ufoegbune, Bruno Lévesque

Research Division, Financial Consumer Agency of Canada

January 2015

Acknowledgements

Numerous colleagues and organizations assisted with the development of this research report. The authors particularly thank the following:

- the US Consumer Financial Protection Bureau;
- the Organisation for Economic Co-operation and Development; and
- the Consultative Group to Assist the Poor.

Executive Summary

Mobile payments (m-payments) are an important aspect of mobile banking, which is a form of retail financial services that is growing rapidly around the world (Continie, Crowe, Merritt, Oliver, & Mott, 2011; Dapp, Stobbe, & Wruuck, 2012; European Commission, 2012). Canadian consumers are increasingly migrating away from branch-based banking towards online and mobile banking. Research suggests that the Canadian market is poised for tremendous growth in the volume of m-payment transactions in the near future (Canadian Payments Association, 2013; Trichur, 2013).

This review will cover recent developments in the regulation of m-payments across the global economy. The focus is consumer protection. We have conducted secondary analyses of markets that closely resemble Canada and/or markets where the m-payment ecosystem is well-developed and regulators have supervisory experience. We studied the problems they identified and their efforts to address these issues. We consider high-level policy issues, such as inter-agency coordination, the purpose and scope of regulation. We also examine the way unique market conditions influence the evolution of m-payment ecosystems. The main purpose of this report is to provide policymakers, regulatory and supervisory agencies, as well as fellow researchers with a broad understanding of the consumer protection issues (e.g., data privacy, disclosure, redress, fraud, and security) and the regulatory efforts which have emerged in foreign jurisdictions as m-payments have evolved.

The current landscape of international m-payment regulation

Restraint and regulation

At this time, most regulators are cautious and hesitant to create new regulation to protect consumers who have begun to conduct payments with their mobile devices. Growth in the volume of m-payment transactions has been steady but slower than projected. Most consider m-payment technology to be in the early stages of its development. Business models are only one or two years old. For these reasons, high-level decision makers in the EU and US are proceeding cautiously. They appear to want to avoid drafting regulation that might discourage innovative firms from developing the m-payment channel or amending the existing rules in a way that favours one type of industry stakeholder or business model at the expense of others. There are concerns that new legislation could work at cross purposes with existing rules or discourage compliance by creating overwhelming complexity.

There are still a number of important developments in terms of new regulation, amendments to existing rules, as well as research and policy proposals which seek to address concerns relevant to m-payments

across the developed and developing world. In spite of a general climate of caution and restraint, regulators have adopted a two-pronged approach: first, industry working groups have been formed to reach agreements on best practices, public commitments, and voluntary compliance guidelines; and, second, new directives, legislation, and regulations have been drafted and passed to address specific concerns about m-payments.

Self-regulation: innovation and interoperability

Regulators have helped to form "working groups" to facilitate dialogue and cooperation between industry stakeholders. Alternatively known as the m-payment "channel" or "ecosystem," the system necessary to conduct payments with mobile devices is complex and comprised of a wide range of industry stakeholders (e.g., mobile network operators, software application developers, mobile device manufacturers, credit and prepaid card networks, financial institutions, and payment service providers).

M-payment ecosystems are built on both "interoperable" technologies (e.g., short messaging service or SMS), which have shared protocols to permit interaction between computer systems, and proprietary technologies, such as the "Google Wallet" software application or a mobile device's operating system (e.g., iOS 7). To develop the m-payment ecosystem, regulators need to facilitate strategic partnerships across industries and promote competition between firms.

In an effort to strike the right balance between competition and cooperation, the U.S. Federal Reserve has convened the Mobile Payments Industry Workgroup, the European Central Bank supervises the European Payments Council, and the Korean Communications Commission formed the Grand NFC Korea Alliance. These working groups share market research, best practices and ideas about interoperability. They work to develop principles that will allow the m-payment industry to supervise itself on a voluntary basis with the assistance of regulatory agencies. These efforts have not been without controversy. In the European Union, some have accused certain stakeholders, in particular large banks, of dominating working group agendas at the expense of less powerful stakeholders, like small retailers (European Commission, 2012a).

Regulatory directives: nonbanks, data harvesting and privacy

Policymakers have drafted amendments and enacted a series of mandatory provisions which address consumer protection issues arising with the growth of m-payments, mobile banking, and e-commerce.

Our review indicates that two types of regulatory tools are emerging. First, although banks have been the gatekeepers of the retail payment system, it is clear that there will be a prominent role in the m-payment ecosystem for nonbanks, payment and trusted service providers, and new third-party firms and contractors. Banks may be exposed to new systemic risks when they enter into strategic partnerships with nonbanks to deliver and settle m-payment transactions. The m-payment ecosystem will only be as secure as its weakest link. Supervisory authorities may have difficulty finding a regulatory burden for nonbanks that is proportionate to the systemic risks they introduce while still restrained enough to encourage new and innovative market entrants. From the perspective of consumers, the wide range of players involved in the m-payment channel can make it confusing when problems arise. Consumers can have difficulty trying to determine which firm is ultimately responsible for settling disputed transactions. In this report

we review steps taken to supervise nonbanks in several jurisdictions. South Korea's Electronic Financial Transactions Act (2007) appears to have the most detailed rules concerning the responsibilities of banks and nonbanks to provide redress to consumers who encounter problems. Second, a number of jurisdictions appear to have decided that their regulatory frameworks will not adequately protect the privacy of the data consumers create with m-payment transactions. Most e-commerce transactions generate a trail of consumer data about browsing behaviour, purchasing habits, and demographic characteristics. When consumers make retail purchases with mobile devices, however, this conventional e-commerce data may be harvested in combination with new information about consumer's geographic location, patterns of movement, calling history, mobile phone subscription, and billing history. Furthermore, consumers typically store personal contacts, photos, messages, and itineraries on their mobile devices.

New "smart" technologies will allow personally identifiable information (PII) and anonymous data to be harvested, combined and processed. This will allow advertisers to create detailed profiles of individual consumers. The profiles can be used to tailor marketing based on the data gathered about consumers. "Behavioural targeted advertising" reaches consumers directly, as they go about their everyday routines. It aims to predict and shape consumer behaviour. This new form of marketing might be relatively benign in some instances, but it could also raise a number of challenging new consumer protection issues.

It appears likely that harvesting data to facilitate new forms of marketing will be essential to the business models of leading m-payment firms. Google is not charging consumers to make transactions or download its "mobile wallet". It appears Google will cover these operational costs in exchange for market share and consumer data, which will strengthen its advertising revenue.

Regulators are trying to balance the need to encourage the growth of m-payment technology with the obligation to protect consumers from new issues that may arise. M-payments enhance consumers' choices. M-payments can allow advertisers to reach consumers with advertising tailored to their tastes and preferences when that advertising is most useful. Targeted advertising might be a key attraction. One way that regulators have found a balance is by allowing consumers to choose how much they participate in targeted marketing. Empowering consumers to make choices can be achieved by requiring informed consent, which means firms need to clearly state the terms of the contract and provide consumers with an opportunity to reject or accept the contract before entering into it.

Experts have praised the consumer protection rules in the EU Data Protection and E-Privacy Directives. The Directives are principles-based, technology neutral, flexible, and adaptive. They allow individuals to divulge personal data when it is in their interests, while ensuring that the harvesting and processing of their data is lawful and fair. However, observers warn that these Directives may not remain sufficient as e-commerce and m-payments continue to evolve (Robinson, Graux, Botterman, & Valeri, 2009).

Table of Contents

1. Introduction

This report provides a summary of international developments in the realm of mobile payments (m-payments) and consumer protection. M-payments are an important aspect of mobile banking, which is a form of retail financial services that is growing rapidly around the world (Continie, Crowe, Merritt, Oliver, & Mott, 2011; Dapp, Stobbe, & Wruuck, 2012; European Commission, 2012). Research suggests that Canadian consumers are increasingly moving away from branch-based banking towards online and mobile banking. In 2010, 19 percent of Canadians surveyed were using mobile banking. The proportion of financial consumers that rely on in-branch banking has declined 30 percent since 2000 to only 17 percent (Canadian Bankers Association, 2012). Experts have observed that the Canadian market is poised for tremendous growth in the volume of m-payment transactions in the near future (Canadian Payments Association, 2013; Trichur, 2013).

This international review is intended to inform government regulators, policymakers, researchers, industry stakeholders, and financial consumers, about the regulatory issues that have emerged with m-payments. The focus is on the potential implications for financial consumer protection. We have researched markets that resemble Canada and markets where the m-payments are established and regulators have supervisory experience. We have conducted secondary research on the problems identified by regulatory agencies, and looked into their efforts to address these issues. Because of the potential for m-payments and mobile banking to transform retail financial services, the research conducted for this report adopts a broad perspective. We consider high-level policy issues, such as inter-agency coordination, the purpose and scope of m-payment regulation, and attempts to solve consumer protection issues like fraud and privacy.

The first section examines m-payment regulation in the United States. The US is similar to Canada in the sense that experts see great potential and yet the growth of m-payments has been slower than anticipated. In response, policymakers in the US have taken the position that passing new legislation for m-payments would be premature at this stage. Regulators have taken steps to amend the existing rules and they continue to monitor a number of issues. Some experts characterize the current regulatory framework as overly complex, which can create challenges because the m-payment ecosystem is also highly complex. Supervising the industry stakeholders that provide m-payments will involve a large number of different regulatory bodies. There is some debate over what aspects of m-payment technology should be shared versus proprietary, and whether regulators have a role in making rules for interoperability. The level at which m-payment technology is shared, or interoperable, will affect the rules that are needed to ensure the security of the data created by m-payments. Finally, there are also unresolved issues related to protecting the privacy of the data provided by, and generated about, consumers who use m-payments.

The second section reports on developments in the European Union. Experts foresee rapid growth in m-payment use in the EU, because of the trend towards electronic forms of payment as well as the rates of mobile phone penetration and mobile banking adoption (Dapp, Stobbe, & Wruuck, 2012). This market readiness, however, has been observed for more than a decade. The growth in the volume of m-payment transactions has been steady but slower than projected (European Commission, 2012). The EU and US

share a lot in common in terms of unrealized market readiness and generally high consumer satisfaction with existing retail payment options, which are reliable, familiar and trusted. The EU has introduced notable regulation for m-payments and mobile banking. We will examine how the EU plans to use m-payments as a vehicle to further harmonize the movement of people, goods, and capital within the "single market." This has led regulators to ask whether fees levied on electronic retail transactions will require new forms of regulation. Our review also looks at the way the EU has addressed issues of data privacy and the role of nonbanks in the m-payment ecosystem.

The third section looks at m-payments and consumer protection in South Korea and Japan. Both markets lead the world in rates of consumer adoption and m-payment transaction volume (OECD, 2012; KPMG International, 2007; Dapp, Stobbe, & Wruuck, 2012). Supervisory agencies have adopted a cautious approach to drafting new regulation and amending the existing framework. We review South Korea's strategy for balancing the promotion of mobile banking with protecting consumers from the risks that arise from m-payments in the Electronic Financial Transaction Act (EFTA) and the E-commerce Consumer Protection Act (ECPA).

Finally in the fourth section we report on the response of regulators to the rise of mobile money in the developing world. We review Safaricom's M-PESA. Launched in Kenya in 2007, M-PESA has emerged as a tremendously successful model for mobile banking in the developing world. Currently, financial sector regulation in developing countries is quite limited, especially with respect to consumer protection. The emergence of mobile money is helping to fill gaps in the availability of financial services. The rise of mobile money has provided an impetus for the construction of a more extensive regulatory framework. Our review tracks the emergence of a number of new consumer protection initiatives.

2. The United States

The US is widely regarded as one of, if not *the*, frontrunner in m-payment innovation (Dapp, Stobbe, & Wruuck, 2012). At the same time, m-payment technology in the US is still seen as being in the very early stages of its development. The market for m-payments in the US and Canada share some important features, such as the trends towards electronic forms of payment, high satisfaction with credit and debit cards, and the high mobile phone and mobile banking adoption rates (Board of Governors of the Federal Reserve System, March 2012; Quorus Consulting Group, 2012). For these reasons, the experience of regulatory agencies in the US can be a valuable source of insight about the potential challenges m-payments might present for consumer protection in Canada.

2.1. Regulatory restraint

At this time, regulators in the US do not recognize an immediate need to create new rules to protect consumers who are making m-payments (Crowe, Kepler, & Merritt, 2012). There is evidence that consumers will begin to use mobile devices to conduct m-payments for goods and services in significantly greater numbers over the next five to ten years.[1] However, the consensus appears to be that m-payment technology is still evolving at a rapid pace. US regulators want to avoid potentially stifling innovation by creating new rules while industry is developing the technology and creating businesses. This position is motivated by a sense that the US market has not been as quick to adopt mobile payments as anticipated. M-payments have the potential to enhance the efficiency of the payment system. Industry stakeholders are striving to convert merchants and consumers from traditional payment options. Observers have cautioned that early regulation stifled innovation in debit card payment networks (Montgomery, 2012)[2]. Finally, regulators have heeded to arguments that even though mobile payments are creating new channels for conducting, clearing, and settling payments, the primary sources of the funds underlying m-payments (e.g., debit and credit cards) are adequately covered by existing regulation for electronic transactions (Crowe, Kepler, & Merritt, 2012).

Regulators have opted to gradually adapt the rules relevant to m-payments in anticipation of new challenges and issues as the technology evolves. This process has been led by the Consumer Financial Protection Bureau (CFPB). Authority over federal laws related to financial consumer protection was transferred to the CFPB in 2011. In part because of the rise of mobile banking and m-payments, the CFPB has adapted the Electronic Fund Transfers Act (Regulation E). The following review of regulation and m-payments in the US will focus on three key issues: regulatory complexity, interoperability, and privacy.

2.2. Regulatory complexity

[1] A recent survey conducted by the U.S. Federal Reserve found that people are increasingly using their mobile phones for banking, payments, budgeting, and shopping. This is particularly true for young persons (18-24) and the unbanked or under-banked; the latter category also contains a disproportionate number of young persons (Board of Governors of the Federal Reserve System, March 2012).

[2] During an exchange on March 29, 2012, at the first session on mobile payments by the Senate Banking Committee, Senators Mark Warner and Richard Shelby agreed that Congress had used a "blunt instrument" when it applied caps on debit interchange fees which potentially limited innovation and growth and that immediate or "heavy-handed" regulation could have a similar effect with respect to mobile payments (Wack, 2012).

The first challenge related to the regulation of m-payments is complexity. M-payments bring together a wide range of industry stakeholders (e.g., mobile network providers, banks and nonbanks, mobile phone manufactures, and software application developers), merchants, consumers, and regulators. The framework of rules governing financial transactions in the US is already complex. It involves a large number of agencies and multiple levels of jurisdiction. Some experts perceive it as overly complex or fragmented (Brown, 2012). M-payments introduce firms that are new to the financial sector and have limited experience negotiating the complex landscape of regulation. These new market entrants are already governed by a separate set of rules in association with their core business. Some observers have argued that the industry convergence created by the rise of the m-payments is going to create a need for "regulatory convergence" (Katz, 2012). In other words, it might be advisable to try and simplify the framework governing financial transactions to accommodate the new market entrants delivering innovative new services like m-payments. According to experts, there are essentially three potential challenges related to complexity and the effort to regulate m-payments. These issues are the potential for ambiguity and gaps, barriers to enforcement, compliance and market entry, and contradictory regulation. The US is addressing these challenges by centralizing authority for federal financial consumer protection under the Consumer Financial Protection Bureau (CFPB).

2.2.1. Ambiguity and gaps

First, experts have observed that the rise of m-payments might lead to ambiguity and gaps in the consumer protection framework. Ambiguity may arise over where the authority of agencies begins and ends. This ambiguity can make regulating new technologies challenging. For example, the Federal Trade Commission (FTC) has authority over many of the firms involved in m-payments (e.g., hardware manufacturers, advertisers, data managers, and software developers). The FTC has primary authority for protecting consumers from fraud, deception or unfair practices, and 15 years of experience monitoring consumer protection rules for mobile technology. The FTC has demonstrated an interest in the lack of privacy disclosure guidelines for mobile applications marketed to children (Crowe, Kepler, & Merritt, 2012). However, the FTC only appears to have jurisdiction over certain types of m-payments, such as direct-to-carrier billing[3].

The Federal Communications Commission (FCC) has supervisory authority over broadband usage. It has a clear interest in the way m-payments will require increasing use of mobile networks. The potential to reach consumers' mobile devices with advertising appears to be important to the business model of firms delivering m-payments. The demands this advertising puts on the wireless broadband technology used to deliver the internet to mobile devices will be of interest to the FCC. Nevertheless, experts note that the FCC does not have the authority to regulate any of the underlying sources of payment. There is some uncertainty over the extent of the FCC's interest and authority over m-payments.

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) may have an interest in supervising person-to-person (P2P) m-payments, which could be used to launder money, traffic

[3] The type of m-payment depends on the underlying source of the funds used in the transaction. Direct-to-carrier billing is one way that consumers can make an m-payment. It occurs when consumers' use their account with a mobile network operator as the source of funds to make a transaction.

drugs, or fund terrorist organizations. The Department of Justice might become involved in supervising m-payments as well. Their interest is related to the laws that govern the acquisition of information about consumers by third-parties (Brown, 2012).

The CFPB has the authority to ensure that every firm providing financial services conforms to federal consumer protection guidelines, rules, and laws. As mentioned above, centralizing authority under the CFPB should address some of the issues related to complexity. The CFPB is reported to have taken the lead on monitoring the adequacy of current regulation and adapting it as technology changes the consumer experience (Crowe, Kepler, & Merritt, 2012). In general, the CFPB has expanded the scope of the definitions in Regulation E to cover m-payments within the existing framework. Regulation E now defines a "financial institution" as any entity that issues an "access device," which includes the mobile devices used to make m-payments (Regulation E, 2011: 1005.2). Some observers have argued that broadening the definitions of key terms will not eliminate ambiguity over regulatory authority. These observers would like to see more precision and the naming of mobile phones in the Act's definition of "access device" (Crowe, Kepler, & Merritt, 2012).

Another issue is that m-payments are regulated by different rules depending on the underlying source of the funds used by the consumer. For instance, debit card payment sources fall under the purview of Regulation E, while credit card transactions are governed by the Truth in Lending Act, or Regulation Z. This means that there might be some ambiguity surrounding the consumer protection for different types of m-payment transactions, even though a single agency responsible for federal law. In sum, the relative complexity of the regulatory framework has created some uncertainty among experts over how consumers will be protected.

Regulatory complexity can also create the potential for gaps in the consumer protection framework. Unlike debit or credit cards, general purpose reloadable (GPR) prepaid cards have been governed only by voluntary industry standards. GPR prepaid cards appear to be the preferred source of funds for m-payments made by unbanked consumers (Board of Governors of the Federal Reserve System, March 2012; Braunstein, 29 March 2012). Aside from young persons aged 18-24, the "unbanked" and the under-banked have been first to adopt m-payment technology, and there is considerable overlap between these two segments of the population. Prepaid cards can be an attractive option to both banked and unbanked consumers who wish to manage their expenditures and avoid using credit. Consumer advocacy groups have raised concerns about the proliferation of (GPR) prepaid cards. The cards are primarily marketed to people with no credit history, or a poor credit rating, who are less experienced, knowledgeable and capable of protecting themselves against predatory terms, such as misleading or deceptive information about fee schedules for transactions, balance inquiries, inactivity, activation, declination, and overdraft (Susswein, 2012). As payments go mobile, it might be necessary to try and improve the financial literacy of unbanked consumers about the risks and benefits associated with these cards. The CFPB is considering extending the consumer protection rules from Regulation E to GPR prepaid cards, which could be an effective response to the gap in the framework.

2.2.2. Barriers to enforcement, compliance, and market entry

The second problem identified in the literature is the potential for increasing complexity to create barriers to compliance, enforcement and market entry. As regulators respond to the issues raised by m-payments, observers have expressed three specific concerns: a) rather than protecting consumers, already difficult to enforce regulation could become even harder to enforce; b) further complexity could make it difficult for newer and smaller firms which may lack the requisite knowledge and/or financial resources to comply; and c) new regulation could create barriers to entering the m-payment market and/or benefit some firms at the expense of others, which might slow innovation and development (Brown, 2012). These concerns are likely behind the cautious approach to regulatory reform in the US.

The firms that are the most sensitive to complex regulation appear to be the software application developers and start-ups that are creating many of the new m-payment platforms. These firms tend to lack experience complying with financial consumer protection rules. They often lack experience working with federal and state-level financial regulators. Generally speaking, software application developers that want to get into the payment business have two options: a) form a strategic partnership with a financial institution, which simplifies the regulatory burden but means sharing revenue; or b) obtain direct supervision by the relevant regulators and incur the substantial time and expense of acquiring and then maintaining licensing fees across all 50 states (Brown, 2012). The considerable costs associated with both options means that many start-ups to fail to even get off the ground. Others fail under the burden of maintenance costs or revenue sharing. Some are bound to fail to acquire licenses in all 50 states or to fully comply with all of the relevant federal regulation (Crowe, Kepler, & Merritt, 2012).

According to observers, the key point is that there is no apparent value associated with increasing the complexity of regulation while there are a series of costs (Brown, 2012). Barriers to entry for developers and start-ups might slow innovation and reduce competition. Uneven compliance by industry stakeholders across states could mean uneven protection for consumers. Certain sources of payment might be accepted in some states and not others. The failure of industry stakeholders to comply or seek licenses could make existing regulation more difficult to enforce. It could also mean that consumer protection varies by jurisdiction, m-payment technology, or type of financial service provider.

2.2.3. Contradictory regulation

The third issue observers have identified stems from the potential for guidelines passed by different agencies to work at cross-purposes. One example might be new rules for person-to-person (P2P) money transfers. P2P remittances may become an important form of m-payments. Mobile technology could provide competition that might bring down the relatively high transaction fees presently assessed on remittances. While fees have not fallen yet, the emergence of mobile remittances still offers consumers a less risky medium for transferring money than cash, which can be more easily stolen, damaged, or lost (Richard, 2012). Regulators would like to encourage the development of mobile remittances. In 2009 at the L´Aquila summit, the G8 Heads of State endorsed the "5x5" objective "to achieve [...] a reduction of the global average costs of transferring remittances from the present 10 percent to 5 percent in 5 years through enhanced information, transparency, competition and cooperation with partners" (Cirasino & Ratha, 2009). Regulators are also mindful of the way P2P could attract persons engaging in criminal money

transfers. Finally, the rules introduced to monitor mobile remittances for criminal activity could work at cross-purposes with privacy laws.

FinCEN has an interest in the evolution of P2P m-payments because they could be used to facilitate money laundering, drug or arms trafficking, or funding terrorist organizations. M-payments significantly increase the speed and ease of money transfers. P2P m-payments allow for more elaborate "disintermediation," which is the layering of money transfers through multiple persons and jurisdictions. Disintermediation could attract people engaging in criminal financial transactions. Criminal money transfers are already difficult to police. It is likely that disintermediation will make detection and monitoring more difficult, as money transfers become disembedded from local markets (Hughes, 10 July 2012).

At the same time, P2P mobile remittances could be easier to supervise than more traditional remittances. M-payments will allow for the creation of an extensive trail of electronic data. This trail could be used to enhance monitoring and enforcement. The CFPB's work to amend remittance regulation has been carried out with the goal of moving the US closer to meeting its commitment to the 5x5 objective. Future regulation of P2P m-payments has to balance the need for sufficient disclosure and record-keeping, with more efficient and cost-effective remittances for global development, as well as the protection of user's privacy. It is apparent that these goals are not necessarily consistent with each other. According to experts, the CFPB's new rules for international remittances successfully balance monitoring and privacy but they might not lead to lower transaction fees because the regulatory burden is greater, which could limit competition and raise administrative costs (Richard, 2012).

2.3. Interoperability

Interoperability refers to the capacity of organizations and systems to work together. Interoperability is created when the rules, standards or practices at the point of interaction between systems (e.g., computer interfaces) or organizations are understood and agreed on so that they can work together in a relatively seamless fashion. Interoperability can exist at a number of different levels. Mobile devices are interoperable in number of ways. For example, they share compliance to the communication protocols governing email and the short messaging service (SMS). Mobile devices are not interoperable at other levels, such as the different operating systems that power them (e.g., Blackberry's 10 OS, Apple's iOS, and Google's Android).

There is a wide variety of firms involved in the m-payment market. There are mobile device manufacturers, telecommunications or mobile network operators (MNOs), banks and financial service providers, data management service providers or "trusted service mangers" (TSMs), large internet-based companies (e.g., Google), and software application developers. These firms have competing interests, limited experience cooperating with one another, and yet each is important to the smooth functioning of m-payment systems.

Regulators in the US are trying to strike a balance between encouraging competition and facilitating cooperation. This means figuring out the level at which m-payments should be interoperable. Greater interoperability could enhance the consumer experience by making m-payments more widely available where consumers purchase goods and services and by standardizing the technology consumers need to

make m-payments. On the other hand, lowering interoperability might increase the role of proprietary technology, which could enhance competition, innovation and consumer choice.

Because m-payment technology is evolving rapidly, regulators have facilitated the formation of the Mobile Payments Industry Workgroup (MPIW) to develop the rules, standards and practices that will form the basis for interoperability. The MPIW is comprised of a wide cross section of major industry stakeholders, such as AT&T, Bank of America, First Data Corporation, Google, PayPal, Visa, and Wal-Mart, which have been brought together by the Federal Reserve Banks of Boston and Atlanta. There is a relatively strong consensus among industry stakeholders that interoperability at the point-of-sale is desirable. Near field communication (NFC) is a set of shared protocols that allow mobile devices to transmit information to merchant's terminals to facilitate m-payment transactions. However, there appears to be less agreement over other aspects of m-payment technology, such as data storage and security.

2.3.1. Point-of-sale

The MPIW has recommended that regulators participate in the process of developing an open m-payment system. MPIW proposes that common rules and open platforms should be enforced to the extent necessary to allow for "a seamless consumer experience" (Continie, Crowe, Merritt, Oliver, & Mott, 2011). In an ideal world, according to the MPIW, the interoperability of m-payments would closely resemble the interoperability of today's global credit card networks. To achieve this goal, a common set of standards would be necessary to allow seamless communication between the various sources of payment (e.g., credit, debit, prepaid), the m-payment platforms (e.g., Google Wallet), the automated clearing houses (ACH), the data managers or TSMs, the MNOs, and the POS terminals. In terms of consumer protection, reaching this goal means harmonizing the regulatory framework for the different payment sources that are combined in m-payment platforms. It will also require common standards for the secure management of personal information and secure transactions at the point of sale (Continie, Crowe, Merritt, Oliver, & Mott, 2011). However, there is a relatively strong consensus among the members of the MPIW that regulatory guidelines should be confined to interoperability at the point-of-sale (POS) at this point.

To enhance the security of m-payments, MPIW suggests that it is important to make the technology interoperable at the point-of-sale. This is particularly true for NFC-based m-payments, which have grown the fastest and were the focus of the MPIW recommendations. Initially there was reason to suspect that credit card payments made with contactless NFC technology were less secure than those made with chip technology and authenticated by consumer's signature and/or Personal Identification Number (PIN) (Wack, 2012a). This perceived risk was balanced against the relatively low dollar limit for contactless transactions. Now that contactless payments are moving to mobile devices with capacities more closely resembling portable computers, the levels of security that can be achieved with m-payments at the POS cannot be matched by other forms of payment. M-payments can be secured by cross-referencing electronic signatures with vast databases, dynamic verification, biometrics, and e-receipts (Andrei, Rusu, Diaconescu, & Dinescu, 2011; Oosting, 2012). Mobile devices and terminals must be held within 10 centimetres of each other and a one-time encrypted code is generated for, and expires upon, completion of each transaction. In short, m-payments can be very secure; however, in order to realize this potential, observers suggest that there is a need for more clarity about the responsibilities of regulators, supervisors, industry stakeholders, and merchants to each other and to consumers.

2.3.3. Secure elements

It has been more difficult to reach a consensus about the interoperability of the technology used to store consumer's data. M-payments require and generate information about consumers. The platforms for NFC m-payments make use of encrypted chips called Secure Elements (SE). The SE is a tamper-resistant chip that stores the user's information (e.g., PIN numbers, card and account credentials, transaction histories). The SE is separate from the mobile phone's OS, hardware and memory, and it is designed to permit only trusted applications (e.g., Google Wallet) to access the mobile phone user's data (Ghag & Hegde, 2012). There are basically three different approaches to SE design: a) the SE can be "embedded" in the mobile device's hardware; b) the SE can be stored in the mobile device's SIM card; or c) memory cards (e.g., microSD), which contain NFC antennas and SEs, can be purchased and inserted into mobile devices. Each design is associated with certain advantages and risks in terms of security. And experts argue that it is equally important for regulators to consider how the different security options also tend to favour different industry stakeholders (Ghag & Hegde, 2012).

It appears that the firm that controls the SE will also control the data generated about purchases and transaction histories, and will thereby stand to realize the highest rate of return. This is not always the case for mobile device manufacturers. Their attraction to embedded SE design stems from the way it creates a strong incentive for mobile device owners to purchase newer models in order to take advantage of improvements made to m-payment platforms. Banks and financial institutions are attracted to storing the SE in memory cards (e.g., microSD) because it would allow them to issue proprietary cards from branches and then harvest and control the data generated about consumers via m-payments. Software application developers like Google prefer to embed the SE in the phone because it gives them control over the data trail generated about customers spending habits in the transaction histories (Ghag & Hegde, 2012). MNOs, on the other hand, favour installing the SE in the SIM Card. The key technical advantages associated with SIM Card-based SE design are that MNOs can protect users with their formidable "over-the-air" security and, in the case of lost or stolen devices, MNOs can remotely lock or unlock SIM Cards when alerted by the phone's owner (Ghag & Hegde, 2012). The problem identified with the SIM Card-based SE design is that it confers an extraordinary amount of power over consumer data to a single industry stakeholder: MNOs. As discussed below, it appears that certain MNOs are willing to exploit their leverage to obstruct or prevent subscribers from gaining access to the m-payment platforms offered by rival firms.

2.3.4. How secure are m-payment wallets?

Along with mobile device manufacturers, industry stakeholders like Google have tended to favour embedding the SE in the mobile device itself. The advantage of this design in terms of objective security is that the consumer's data is securely encrypted along the entire path, from storage to processing and back again. However, security experts argue that the capacity of mobile devices to support complex encryptions is fairly limited (Hoog, 2011). The devices have limited processing power and the storage capacity of the SEs is negligible (Hoog, 2011). For this reason, Google Wallet stores transaction histories, account balances, available credit, expiry dates–almost everything beyond the PIN and the first 12 digits of the credit card numbers–outside of the SE. This can increase the potential for personal data theft (Hoog, 2011).

Android is the OS that powers the majority of mobile devices. As a result, Android has become the most popular target for malware, viruses, Trojan horses, harmful and malicious software applications which can be installed on mobile devices by third parties for the purposes of stealing data, damaging the mobile phone, or using it for unauthorized purposes (e.g., fraudulent purchases). One study of limited scope managed to collect 1,200 samples of Android malware between the August 2010 debut of a new version of the OS and October 2011. The authors estimate that Android's share of mobile device malware is approximately 46 percent. The best mobile security software found only 79.6 percent of malware, while the worst detected only 20.2 percent (Zhou & Jiang, 2012).

Google Wallet prepaid cards have proven vulnerable to infiltration without "rooting" or malware installation. Security experts demonstrated that when the data was cleared from the Wallet's settings menu it prompted whoever launched it next to enter a new PIN number. This design flaw left the funds stored on Google Wallet's prepaid card highly vulnerable to fraud (Ghag & Hegde, 2012). The NFC antenna also provides a surprisingly broad point of entry to "proximity attacks." Hackers can enter through the peer-to-peer interface and take the mobile phone user's browsing history, files, and documents, when the attacker is within a range of 10 centimetres (Miller, 2012).

Google has responded to these security threats in a number of ways. The Google Wallet prepaid card was discontinued in October 2012 when the aforementioned design flaw was made public. The threat of proximity attacks is reduced by not powering the NFC antenna when the screen is off. 4-digit PINs are required to view the cards in Google's virtual wallet once the application is locked, and it locks automatically after a short period of disuse. If the mobile device is stolen, the user can remotely disable the Google Wallet application online to prevent it from being used for fraudulent purchases. Furthermore, the latest version of Google Wallet makes use of a cloud/SE hybrid design, storing the debit and credit card credentials on Google's internet servers rather than outside the SE on the device. Only the prepaid card and Wallet ID remain on the phone and both are stored in the SE. Generally speaking, the objective or technical security of Google's m-payment platform is actually quite high. The reports of potential security threats reviewed above have decreased the perceived or subjective security associated with the Wallet. Critics have urged Google to respond to the perception of it as a large corporation with a "start-up" mentality that does not take its users' security seriously enough. If properly set up, the Google Wallet remains most vulnerable to attack from persons who are acquainted with the owner and can thereby either acquire the owner's PIN or gain access to the mobile device while it is unlocked (Ghag & Hegde, 2012).

Initially, Verizon Wireless would not allow their customers to download the Android OS updates required to use the Google Wallet. While Verizon pointed to the security concerns described above, industry observers suspected that there were two more important concerns. First, Verizon is involved in a joint venture called "Isis Mobile Wallet" with AT&T Mobility and T-Mobile USA. -Isis was announced before the Google Wallet but the Isis platform did not reach test markets in Austin and Salt Lake City until October 2012 (Olivarez-Giles, 2012). Instead, Google was the first firm to release its m-payment Wallet in the US market. In September 2011, the Google Wallet was launched on a single phone model, the Sprint Nexus S 4G, which ran Google's own OS (i.e., Android) and was carried only by Sprint. Second, competitors have expressed concern over the way Google uses proprietary technology to process the Wallet user's data.

This technology would confer control over the data to Google. Industry observers speculated that Verizon's delay over enabling Google Wallet on its networks was motivated by the failure to reach a suitable revenue/data sharing agreement, since AT&T and T-Mobile allowed the Wallet and did not raise similar concerns about its security. Verizon has since changed its position and now permits the requisite updates to Android OS mobile devices on its network. This example demonstrates how security and interoperability are connected.

2.4. Privacy issues: Data harvesting and consumer protection

Of all the issues m-payments raise with the existing framework of consumer protection rules, privacy is arguably the most complex. For industry stakeholders there are essentially three sources of revenue from m-payments: a) the sale of software applications or m-payment platforms; b) charging transaction fees for processing m-payments; and c) data harvesting and advertising. Because secure, efficient, and reliable payment options are well-established in the US, it is likely that revenue earned from data harvesting and targeted advertising will be an important part of m-payment providers' business models (Hughes, 10 July 2012). The growth of new forms of advertising and data processing might create challenges for regulators in charge of protecting financial consumers.

Google, for example, currently allows customers to download the Wallet for free. They do not charge consumers for processing their payments (Google, 2013). Their business model appears designed to capture market share. It also suggests the potential to earn substantial revenue by gathering data about consumers as they make m-payments. The data can be used to reach consumers directly with customized advertising on their mobile devices. Google intends to realize a profit from the m-payment channel mainly through data harvesting and advertising. This model is promising enough that they are willing to forgo revenue from transaction charges and the sale of their software application for the time being.

The privacy issues raised by m-payments are complex. Regulators in the US appear to want to strike a balance between two responsibilities. First, the regulators have a duty to protect consumers' right to opt out of data harvesting and/or receive adequate disclosure about how their data is being harvested, processed and used. On the other hand, regulators perceive a responsibility to facilitate the development of the m-payment ecosystem and provide consumers with more choices by allowing industry stakeholders to compete for commercial rewards. From the perspective of consumers, the personalized or "smart" marketing (e.g., behavioural targeted advertising) facilitated by data harvesting can be seen as an advantage m-payments have over more traditional payment methods. Some consumers will be attracted to m-payments because of the convenience of receiving advertisements customized to their tastes and preferences. Observers have noted that protecting consumers while also allowing them to participate in this new kind of marketing may require modifying privacy and disclosure rules. Adapting the existing framework or developing new rules for privacy protection will be challenging. There are a large number of industry stakeholders, regulatory authorities, data channels and storage sites, to consider. And there are a number of different ways to harvest, process and employ data through marketing and advertising applications. Reforming the existing framework might not be sufficient. Some argue that a new code may be required to adequately protect consumers' privacy (King & Jessen, 2010).

2.4.1. Data harvesting and behavioural targeted advertising

To understand the challenges m-payments might create for US regulators, it is crucial to briefly consider the essential differences between market segment research and consumer profiling. Advertisers have been using statistical analysis and market research to target specific segments of the population for a long time. However, King and Jessen (2010) have observed four important changes in consumer analysis and marketing. Together these changes represent a new paradigm called behavioural targeted advertising, which will grow in importance along with m-payment technology.

First, m-payments allow industry stakeholders to harvest new forms of data and bring it together with more conventional information gathered about consumers. Typically, data trails about browsing behaviour, purchasing habits and demographic information (e.g., names, mailing addresses, phone numbers, etc.) are created as consumers use the internet. Mobile devices can generate additional personal data about geographic location, movement, mobile phone subscriptions, billing information, and calling history. Moreover, people typically store personal contacts, messages, itineraries, photos, and a range of other consumer goods, like music, in their mobile devices. In sum, m-payments will generate a much wider range of data about consumers, which can be combined with more conventionally gathered data for the purposes of market research and advertising (King & Jessen, 2010).

Second, new "smart" technologies will be used to mine this information from data warehouses. The data analysis will be performed by computers automatically, or nearly automatically, with limited human intervention. Consumer profiling does not depend on human intelligence but rather computer programs designed to mine warehouses automatically. These programs can discover unexpected correlations between data about consumers' characteristics and forms of consumer behaviour (King & Jessen, 2010).

Third, these computer-generated analyses are capable of producing highly individualized consumer profiles. This has the potential to blur the lines between personally identifiable information (PII) and anonymous data. US privacy law defines PII as data that can be used to identify, locate, or contact a single person. Anonymous data does not enable identification. Data analysis based on consumer profiling is far more individualized and personal than analysis based on market segment research. The volume of highly specific data harvested from mobile devices is greater and more sophisticated techniques are used to mine this data from warehouses. Profiling based on m-payment data harvesting allows for advertising targeted at specific individuals based on their unique personal characteristics. Market segment research creates knowledge about broader categories of consumers. Consumer profiling allows for the behaviours, preferences, tastes and attitudes of individuals to be profiled with a higher degree of specificity. Correlations can then be found between an individual's characteristics, behaviour, and the profiles of other consumers to create more sophisticated market categories. However, the basic unit of the targeted advertising enabled by m-payments will be individual consumer profiles, not market categories. Marketing through m-payment technology will target particular individuals rather than a type of person (King & Jessen, 2010).

Fourth, consumer profiling based on m-payment transactions will not be limited to descriptive analysis. The purpose of behavioural targeted advertising is to predict and shape the behaviour of individual

consumers in real time. Websites that display advertising often install "cookies" on users' computers to create a profile of the consumer's browsing habits. This profile is used to generate more compelling advertising. The key innovation enabled by m-payments will be the way marketers can reach consumers directly as they make and consider purchases. This type of real-time behavioural advertising might actually shape consumers' choices as they are making them (King & Jessen, 2010). One benign example might have a consumer departing for their afternoon break and then finding a coupon sent to their mobile phone which offers a discount on a new product at their local coffee shop if the person makes their customary purchase. Less benign examples could involve the targeted marketing of more controversial products, such as fast food, to consumers with chronic conditions, like type-2 diabetes. In sum, the growth of m-payments will enable the rise of behavioural targeted advertising. This new form of marketing is premised on the harvesting of a wide range of data about consumers, automated computer technologies that mine and analyze the data, the generation of highly individualized consumer profiles, and advertising designed to predict and shape the behaviour of targeted consumers.

2.4.2. Data protection, personal autonomy and liberty

M-payments and behavioural targeted advertising raise two issues related to the protection of consumers' privacy: a) data protection and b) personal autonomy and liberty (King & Jessen, 2010). In terms of data protection, most of the concern surrounds the collection and disclosure of PII, which is data that allows for a single person to be identified, contacted, or located. Consumers need adequate notice, the ability to offer informed consent, and the option to decline to have their PII harvested and used for commercial purposes. Behavioural targeted advertising also exposes individuals to new risks concerning identity theft and the general security of their PII. There is the potential for the profiling enabled by m-payments to create a pervasive and less than transparent web of surveillance, as consumer behaviour is increasingly tracked, monitored, and processed. Finally, there is the potential for consumers to be exposed to unfair or deceptive business practices (e.g., discriminatory pricing) as marketers aspire to shape consumers' choices while they are being made (King & Jessen, 2010).

M-payments might create challenges for regulators that are responsible for protecting personal autonomy. In part this because behavioural targeted advertising can create asymmetries of information between marketers and consumers. When consumers do not know what information is being gathered about them, which firms are gathering it, and how they are using it, there is greater potential for consumers to be manipulated. For example, this kind of advertising could be used to target vulnerable populations with unhealthy food, medications, or high-interest consumer loans (King & Jessen, 2010). Consumers need to know why they are receiving these new advertisements in order to make informed and responsible decisions.

2.4.3. The regulatory framework for the protection of consumer privacy

US law recognizes privacy in the broad sense of personhood, as well as a fundamental right to be protected from commercial or government intrusion. However, experts have argued that there is no comprehensive regulatory framework to protect consumers' privacy from data harvesting, behavioural targeted advertising, or manipulative marketing practices. Observers have indicated that the complexity of the regulatory framework will be an issue when adapting privacy rules in response to m-payments (Brown, 2012; King & Jessen, 2010). The US does not have a single agency with the ultimate authority to supervise

and enforce privacy law. The applicable regulations vary based on the industry stakeholder, the type of data, the manner in which it is warehoused, and the use of the information (Brown, 2012). The FTC has most of the supervisory authority for the rules that safeguard the privacy of consumer data. These rules are complex. For instance, there are minimum standards for harvesting data from children under the age of 13 set out in the Children's Online Privacy Protection Act (COPPA, 1998). The harvesting of data about consumers is governed by Gramm-Leach-Bliley Act (Financial Services Modernization Act, 1999). Data collected by credit reporting agencies about consumers' credit history must be managed in a manner consistent with the Fair Credit Reporting Act (FCRA, 1970) and the Fair and Accurate Credit Transactions Act (FACTA, 2003). These four acts are supervised by the FTC. However, rules for the data collected by health care providers are provided by Title II of the Health Insurance Portability and Accountability Act or the "Administrative Simplifications" provisions (HIPAA, 1996), which are enforced by the U.S. Department of Health and Human Services' Office for Civil Rights.

State laws add more complexity, as does the relationship between state and federal acts. Laws have been passed by 46 states which require consumers to be notified when information about them is shared with third-parties. The Department of Justice may also have jurisdiction to enforce laws about the disclosure of consumer data to third-parties. California has broader definitions of PII and forbids retailers from requiring or requesting PII at the point-of-sale. The CFPB has some interest in supervising privacy law pursuant to its acquisition of authority for Regulations Z and E. Finally, corporations like Visa and MasterCard have their own rules which prohibit merchants from disclosing certain information about transactions to unregistered third-parties (Brown, 2012). To the extent that the existing framework is guided by an overarching objective, it is the principle that consumers should be informed and able to exercise a measure of control over information gathered about them for purposes of marketing (Brown, 2012).

2.4.4. Will the law protect consumer's privacy in the m-payment channel?

The complexity of the rules can create challenges for protecting consumers' privacy. For example, the Telecommunications Act (1996) gives the FCC the authority to protect consumers when MNOs harvest their data, such as outgoing call histories and geographic location. The data collected by MNOs about a consumer's telephone calls (e.g., the time, date, destination and duration), the consumer's network subscription, and the information that generally appears on a consumer's phone bill, are stored in the Customer Proprietary Network Information (CPNI) data warehouse. The CPNI is regulated by the FCC. However, the Act's definition of personal data excludes a mobile customer's phone number, address, and name, which means that this information is afforded very little protection. Furthermore, non-MNOs, advertisers, and websites mining the data in the CPNI warehouse are not currently supervised by the FCC (King & Jessen, 2010). This represents an important gap in the existing consumer protection framework.

Observers have also suggested that self-regulation can create a disincentive for industry stakeholders to adopt detailed policies for the protection of consumers' privacy. Generally speaking, businesses in the US are permitted to market their products as they see fit so long as they do not engage in deceptive business practices or violate the law (King & Jessen, 2010). The FTC has authority over deceptive business practices. It has not defined consumer profiling or behavioural targeted advertising as unfair or deceptive. The FTC has not asked companies that profile to adopt a specific set of privacy policies. As a result, the most

efficient way for companies to minimize their legal exposure is to not adopt a privacy policy with detailed rules about consumer profiling or targeted advertising. If companies decide to adopt privacy policies, there is a strong incentive to write the policy in such a way that gives the company broad scope to generate and share data, create profiles, and conduct behavioural targeted advertising. Some observers suggest that these incentives could work to undermine the protection of consumer's privacy (King & Jessen, 2010).

3. The European Union

M-payment adoption rates in the European Union (EU) have not reached the heights projected by experts. The shift towards e-commerce, cashless payments, and smart mobile devices has created the optimal market conditions for more widespread use of m-payments (Ondrus, Lyytinen, & Pigneur, 2009). In 2010, there were only 7.1 million m-payment users in Western Europe compared to 62.8 million users in the Asia/Pacific region (European Commission, 2012).

This review will cover four key issues. First, regulators are interested in facilitating the growth of m-payments because they see it as a way to further harmonize the market for retail payments across the EU. Second, the challenges associated with the effort to harmonize payment products, technical requirements, interoperability and the m-payment infrastructure across the EU. This has been addressed through voluntary, self-regulation under the Single Euro Payments Area (SEPA) initiative. Third, the binding and relatively comprehensive laws for consumer privacy and the protection of personal information introduced with the Data Protection and E-Privacy Directives. Finally, the Payment Services Directive (PSD), which provides the legal framework for defining the entities that can provide payment services as well as their conduct, will be examined.

3.1. Regulatory goals: develop m-payments to create a "single market" for retail payments

After more than a decade of trials and pilot projects, the key issue for regulators remains how to facilitate greater consumer adoption of cashless/electronic payments in the EU. Regulators want to know how to encourage the growth of the m-payment ecosystem. The goal of the European Commission is to create a seamless "single market" for retail payments in the EU They want retail payments to cross national political boundaries with the same ease as people and businesses. At the same time, observers have noted that the existing rules are already quite complex. There is a concern that introducing new regulation for m-payments might increase complexity without enhancing the effectiveness of the rules. New regulation could also stifle innovation and/or unduly favour one type of industry stakeholder at the expense of others (European Commission, 2012a).

The objectives and challenges for the regulators supervising m-payments in the EU are similar to their counterparts in the US. There are important differences as well. The EU has made progress towards harmonizing retail payments by creating a detailed and binding framework of rules for consumer protection in the m-payment channel. The EU has also clarified the status and obligations of the non-bank payment service providers, which are important to the delivery of m-payments. EU regulators are motivated to encourage the growth of m-payments because they see this work as contributing to the broader goal of creating a single-market for retail payments across

3.2. Harmonization: SEPA, self-regulation and transaction fees

3.2.1. SEPA

In an effort to harmonize regulations for retail payments, the EU has opted for a voluntary system of self-regulation for e-commerce and m-payment channels. The SEPA initiative to enhance self-regulation is steered by the European banking sector through the European Payments Council and the European

Central Bank (European Central Bank, 2006). The purpose of SEPA is to create a set of rules and guidelines regarding technical standards, interoperability, and security. These rules will then be adapted and adopted by national jurisdictions with the aim of creating a safe and efficient "single market" for retail payments. Progress towards this aim has been uneven.

There are four SEPA frameworks relevant to the self-regulation of m-payments. SEPA introduced a pan-European regulatory framework for credit transfers (SEPA Credit Transfer or SCT) in 2008 along with a framework for direct debit payment schemes (SEPA Direct Debit or SDD) in 2009. The European legislature adopted these frameworks in February 2012 (European Payments Council, 2012).[4] When the source of funds for m-payments are credit and debit cards these payments will be regulated by the SEPA Cards Framework, which was first introduced by the EPC in 2006. Most industry stakeholders have taken the position that SEPA SCT, SDD, and the Cards Framework, are sufficient to govern m-payments (European Commission, 2012a). However, the EU has introduced a new instrument specifically for m-payments. The Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines (MCP IIGs) was published in November 2011. Its purpose is to facilitate and promote the development of common standards and best practices for industry stakeholders. To date voluntary compliance with the SEPA Cards Framework and the Guidelines has not kept pace with the higher rates of industry conformance to SCT and SDD (European Commission, 2012; Jones, 2009).

3.2.2. Self-regulation

The SEPA frameworks are meant to provide industry stakeholders with tools for achieving self-regulation (European Payments Council, 2012). MCP IIGs provides recommendations for commitments on interoperability and technical standards. Compliance with these guidelines is voluntary for card schemes, card issuers, acquiring banks, trusted service managers (TSMs). The first priority is to make card payments simpler and safer for consumers and merchants. Regulators also want to facilitate competition and cooperation between industry stakeholders. Towards the latter objectives, SEPA's guidelines for m-payments are highly similar to the "road map" put forward by the MPIW in the US Both promote open standards and interoperability over proprietary and "closed" m-payment solutions. One difference is that SEPA does not recommend interoperability at the level of the Secure Element (SE). Their preference is to set common standards at the level of the software application in the consumer's mobile device. In other words, consumers should be able to access all of their m-payment services on a single mobile device (European Payments Council, 2012).

According to observers, there are several challenges associated with the SEPA initiatives. First, the protections and procedures for consumers and merchants engaging in cashless retail transactions vary across the EU. National adaptation of SEPA's guidelines has prevented full harmonization. Ambiguity persists over what compliance means. As result, industry compliance remains uneven (Jones, 2009). There is also the potential for consumers to be mistaken or unaware of their rights and protections, as they cross

[4] SDD and SCT were adopted by the E.U. in February 2012 with Regulation (EU) No. 260/2012 and the amendment Regulation (EC) No. 924/2012. The deadline for the 27 European member states to bring their national standards into compliance with SCT and SDD was 1 February 2014. The deadline for the non-EU states that adhere to SEPA (i.e. Switzerland, Monaco, Mayotte, Saint Pierre and Miquelon) to conform their national laws to SCT and SDD is 1 March 2016 (European Payments Council, 2012).

borders and make retail payments in different jurisdictions. The primary point of contact in the case of an authorized transaction can vary depending on the mobile payment platform, the payment service provider, the issuing or acquiring banks, and the national jurisdiction of the point-of-sale.

Experts have indicated that it is also possible that regulatory complexity has hindered the achievement of the European Payments Council's primary goal of creating a seamless "single market" for retail payments. At the present time, people and businesses are able to move across borders in the EU with greater ease than card-based retail payments. Despite the existence of pan-European guidelines, standards, and best practices, the effort to integrate the market for cashless payments has lagged behind. Domestic debit card schemes, for example, are usually not accepted as a source of payment for goods and services outside of the member state where a consumer's financial institution is located.

The overwhelming majority of industry stakeholders that responded to the European Commission's Green Paper on m-payment regulation argued that the lack of integration is not the result of a lack of cooperation between firms (European Commission, 2012a). Some banks have claimed that competition laws are not consistent with SEPA's interoperability guidelines. Most payment service providers argue that the integration of the retail payment system has been slowed by the large number of differences in the rules across national jurisdictions. EU members have different standards and rules, settlement and clearing protocols, processing requirements, technical specifications for terminals, along with different domestic card schemes, licenses, applications, and bilateral interchange agreements (European Commission, 2012a). While there is little support for mandatory harmonization, it appears evident that instruments of self-regulation have yet to create a seamless market for consumers.

Third, the complexity of the regulatory landscape means that fraudulent use of payment cards remains relatively high, especially for remote m-payments (European Commission, 2012). Since credit cards will serve as the underlying source of funds for a large proportion of m-payments, the way the current landscape allows for the persistence of relatively high levels of credit card fraud is an important concern.

Finally, even though most agree that the industry should regulate itself, the absence of an independent decision-making body to oversee the drafting of SEPA's frameworks has been widely criticized. The majority of industry stakeholders expressed concern that SEPA unduly favours the interests and priorities of banks (European Commission, 2012a). Some of the new payment service providers have argued that incumbents are foreclosing access to the existing transaction settlement infrastructure. Newer firms are more likely to favour obligatory regulation, mandatory harmonization, and higher levels of interoperability (European Commission, 2012a). National governments and smaller banks have expressed concern that low-cost domestic debit channels could be squeezed out of the payment market by the two dominant credit card networks. In other words, Visa and MasterCard could effectively form a duopoly over retail payments, if the harmonization of rules does not account for the interests of the full range of industry stakeholders. Merchants want the authority to choose their acquiring bank from the card network or they want SEPA to be used to create a central acquiring bank (European Commission, 2012a). Consumers, merchants, and software developers have argued that SEPA's governance structure should be changed. They want ultimate authority to rest with the European Commission and the European Central Bank rather than European Payments Council, which is seen as favouring the interests of banks.

Credit card companies and payment service providers have argued that stakeholder participation should be more balanced and that their representation should be greater.

3.2.3. Transaction fees

One reason why the adoption of the SEPA Cards Framework has been delayed is the controversy over whether there is a need to regulate transaction fees and, specifically, interchange fees. Every time a consumer pays with a card–unless that card is part of the merchant's "closed-loop" prepaid network–a series of transaction fees are exchanged between cardholders, merchants, banks, and payment card network operators.

Most payment card networks are four-party systems (Borestam & Schmiedel, 2011). There are four types of fees in this arrangement. First, the consumer who holds the card will make monthly payments to their issuing bank, along with interest on any outstanding balance, and some cases an annual fee. Second, the merchant that accepts the consumer's card payment sends a fee called a merchant service charge (MSC) to their acquiring bank[5]. Third, when the issuing bank settles the cardholder's purchase by sending payment to the merchant's acquiring bank, the issuing bank receives an interchange fees from the acquiring bank[6]. Fourth, the payment card network operator receives "switch fees" or "assessments" from both the acquiring and issuing banks (Borestam & Schmiedel, 2011).

The fees assessed on transactions in payment card networks have become controversial in the EU for a number of reasons. As consumers increasingly choose to make card-based electronic payments, the revenues banks and payment card network operators earn from transaction fees have grown considerably and attracted more attention as a result. There are also concerns about competition because the fee schedules are generally set by the payment card network operators and the market is dominated by two operators (i.e., Visa and MasterCard) (Martin, 2010).

Interchange fees have been subjected to the most scrutiny. In part, the attention is due to the significant variations in the interchange fee rates between national jurisdictions. EU policymakers are also concerned about the higher interchange fees that are levied on transactions when the issuing and acquiring banks are located in different national jurisdictions. Policymakers view these disparities and extra surcharges as barriers to the creation of a seamless "single market" for retail payments (European Commission, 2012). On the other hand, payment network operators argue that these disparities and surcharges reflect the costs of settling transactions within and between different national jurisdictions (European Commission, 2012a; Haas, 2012). The EU General Court ruled to fix the interchange fee on cross-border settlements at 0.2% for debit card transactions and 0.3% for credit card payments in May 2012 (European Commission, 2012c).

[5] Because the acquiring bank will debit the MSC from the total purchase amount when reimbursing the merchant, the MSC is often referred to as the "merchant discount" or "discount rate".

[6] The interchange fee is also known as a multilateral interchange fee (MIF) when the fee schedules are arranged by the payment card network operators for a number of different acquiring and issuing banks. If the interchange fee schedule is set out in a contract between one issuing bank and one acquiring bank, it is referred to as a bilateral interchange fee.

The debate over interchange fee regulation is relevant to consumer protection and m-payments for other reasons as well. First, experts have observed that the four-party payment card system can lead to higher interchange and merchant service fees when competition intensifies. Payment card network operators often try to attract consumers and persuade them to use their cards with increasingly generous reward programs. Because payment card network operators set the transaction fee schedules, the cost of enhanced reward programs can be recouped by increasing the fees merchants pay to have card-based payments settled. Interchange and switch fees are ultimately drawn from merchant service charges. Contracts between merchants, acquiring banks, and payment card network operators generally forbid merchants from discriminating between higher cost premium credit cards and more basic cards from the same network. As card networks compete to attract more consumers, they can drive up the costs associated with accepting card-based electronic payments for merchants (Evans & Mateus, 2011; Hayashi & Weiner, 2005). Because competition in the payment card market has tended to increase interchange and merchant service fees, there is a possibility that fees could also rise as m-payment providers strive to attract consumers to a new payment platform.

Merchants have filed numerous complaints about the fairness of transaction fees (Evans, 2011). In the EU, consumer advocacy groups and merchant associations have argued that transaction rates are not justifiable given the low cost of maintaining and operating the network used to settle debit and credit card transactions. It is important to recognize that this kind of cross-subsidy in which merchants subsidize the costs associated with the consumers' choice of payment is typical of two-sided markets. While the credit card market is concentrated, operators still need to compete with other forms of payment (e.g., cash, debit, closed-loop and prepaid cards). The need to ensure that merchants continue to accept credit cards should also put downward pressure on transaction fees. Nevertheless, it is important to consider that the competition introduced to the market by m-payments might not necessarily lower transaction fees for merchants. Rising transaction fees can also translate into higher prices for consumers, to the extent that merchants are able to pass through the rising costs associated with merchant service charges. This pass through is not highly transparent, as many consumers are unaware of the transaction fees associated with different payment cards and the way these fees might impact prices (Haas, 2012). There can also be cross-subsidies between different classes of consumers, as only consumers who have premium payment cards will benefit from the reward program enhancements but merchants raise retail prices for all consumers (Bergevin & Zywicki, 2012). This arrangement has been interpreted as a regressive transfer of wealth because lower income consumers who pay with cash, debit or conventional credit cards are subsidizing the more generous rewards earned by premium card holders who meet the higher income requirements associated with most rewards cards. Regulators may wish to mindful of these cross-subsidies as m-payment grow in popularity.

Finally, there is growing concern that interchange fees and the contracts that set out the fee schedules are barriers to the entry of newer, smaller, and more innovative payment service providers. This has the potential to reduce the competitiveness of the payment services market, which could be detrimental to merchants, consumers, and the broader economy. Barriers to entry can also reduce innovation. Electronic payments are not just important for furthering harmonization. EU policymakers also consider electronic payments to be a more efficient means to circulate money throughout the economy. Lawsuits have been

filed in the US against payment card network operators on behalf of large retailers for anti-competitive practices. EU anti-trust officials have been investigating Visa's interchange fee schedules for more than four years and they filed a preliminary notice of objection in July 2012. The European Commission (EC) claims that Visa's MIFs restrict competition between banks and infringe on EU rules prohibiting cartels (European Commission, 2012b). It is has been argued that barriers to market entry will hinder the development of the m-payments, while anti-competitive practices could prevent the m-payment channel from providing consumers with a low-cost alternative. On the other hand, the participation of Visa and MasterCard could also spur the adoption of m-payments by consumers, because these payment card network operators have built reputations for safety and reliability.

3.3. Data protection and privacy

Harvesting and processing data about consumers and their transactions is integral to the m-payment business. Legal regulations for data protection and privacy rights in the EU are highly developed. The EU framework is somewhat stronger than OECD guidelines (Greenleaf, 2012). Two directives protect consumers' privacy when they make m-payments: the Data Protection and E-Privacy Directives. Both are required to be adopted by member states through national legislation (King & Jessen, 2010). In addition, most EU members have also signed on to Convention 108, which is an international treaty on data protection (Council of Europe, 1981). Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) provides individuals with further rights to privacy, except when interference may be required in the interests of national security, public safety, or economic well-being (ECHR, 2010). Finally, the Charter of Fundamental Rights of the European Union (E.U. Charter) indicates in Article 8 that "Everyone has the right to the protection of personal data concerning him or her," "Such data must be processed fairly," and "Everyone has access the right of access to data which has been collected concerning him or her, and the right to have it rectified" (EU Charter, 2000). These treaties inform current efforts to modernize privacy and data protection. This review will focus on the Data Protection and E-Privacy Directives, because of their level of sophistication and relevance to the EU's strategy for protecting consumers who have begun to make m-payments.

The Data Protection Directive is a principles-based regulatory framework that must be adopted, and can to a certain extent be adapted, by national jurisdictions within the EU (Directive 95/46/EC). The Directive is comprised of eight core principles. The first and guiding principles are that of lawfulness and fairness. While the former term is self-explanatory, fairness is interpreted to mean that the entities harvesting, processing and controlling personal data (i.e., "data controllers") must take into account the interests of the individuals (i.e., "data subjects) who are having data about them gathered. The concepts of lawfulness and fairness inform and take precedence over the principles that follow (Bygrave, 2000).

The second principle is "finality" which means that an individual's data may only be collected for legitimate purposes. The purpose must be specified and made explicit. Data can only be used in ways consistent with the stated purpose. (King & Jessen, 2010). The third principle is that of "minimalism" or "proportionality," which means that the data collected should be limited to the volume necessary to achieve the purpose for which the data was originally collected. Fourth, the principle of "information quality" stipulates that the data harvested and processed should be reasonably current, accurate, and valid for what the data is intended to represent. The "quality" principle also calls for a system of regular

checks to confirm the data's validity. The fifth principle concerns an individual's rights to "participation and control" over the data gathered about them. There are two types of provisions. On the one hand, there are rules requiring the data controller to make basic information about their data harvesting and processing practices available to the relevant supervisory authorities, and then there are rules that oblige the regulatory authorities to make this information available in a public register. On the other hand, there are guidelines requiring data controllers to directly contact the subjects of the data, to make subjects aware of the procedures used to harvest and process the data, and to secure the informed consent of data subjects before proceeding. The sixth principle stipulates that data controllers may only disclose data to third parties under very specific conditions. At an absolute minimum, the informed consent of the subject is required before data gathered about them can be disclosed to third-parties. Principle seven requires data controllers to take all necessary and reasonable steps to ensure data security by preventing accidental destruction, unauthorized access, or alteration. Finally, the eighth principle addresses "sensitivity" and it requires data controllers take extraordinary measures to ensure the most stringent security of especially sensitive data (Bygrave, 2000; King & Jessen, 2010).

The main regulatory framework for protecting the privacy of information communicated by individuals across electronic channels in the EU is the E-Privacy Directive (2002/58/EC). This act extends the protections offered by Data Protection Directive (95/46/EC). The E-Privacy Directive specifically targets mobile network operators (MNOs) and internet service providers (ISPs). It requires them to comply with all of the core principles that can be applied from Data Protection Directive, such as "informed consent." More specifically, the Directive is intended to ensure that advertisers receive informed consent before sending unsolicited advertisements to consumers' mobile devices. The Directive's definition of personally identifiable information (PII) includes data harvested from consumers' mobile devices about internet traffic, browsing histories, and geographical location. In order to use this data, the Directive requires MNOs and ISPs to transform traffic and location-based data into anonymous data, to notify consumers that the data is being harvested and processed, and to obtain informed consent. Finally, the Directive empowers consumers to opt out of HTTP cookies, tracking software, and other devices that can be placed on their mobile devices in order to gather data about their activity over the networks of MNOs and ISPs.

Gaps have been identified in the E-Privacy Directive. For example, it does not address certain forms of person-to-person marketing. Advertising sent indirectly through natural or legal persons instead of directly to consumers from businesses will likely be exempt from the privacy rules. The Directive will not regulate individuals who send electronic communications to other consumers to market goods or services that the other consumer owns or has purchased in the past (King & Jessen, 2010). This exemption could open the door to some unsolicited advertising from third-parties, which is a form of marketing that has been growing in importance recently. Advertising sent indirectly by consumers who use "like" or "recommend to a friend" applications on the popular social media website Facebook would be exempt. There is also ambiguity over how Data Protection and E-Privacy Directives will be combined to work in concert on issues like "secondary identifiers," IPs, and HTTP cookies.

3.4. The Payment Services Directive, nonbanks and payment institutions

The Payment Services Directive (2007/64/EC) is a regulatory initiative of the European Commission's Directorate of the General Internal Market. The Directive has two main objectives. First, it is designed to

help create a single market for electronic retail payments across the EU. To help achieve this goal, the Directive removes barriers of entry and guarantees fair market access to new payment service providers (e.g., retailers, MNOs, and money remitters). It aims to do this by harmonizing the regulatory landscape across the 27 member states.

The Directive creates broad authorization for Payment Institutions (PIs), which is a new way to define industry stakeholders in the m-payment market as objects of supervision and regulation. PIs must meet capital and risk management guidelines and apply for authorization in the EU member states where they intend to offer payment services. Once these obligations are met, PIs can operate across the EU without further authorization from additional supervisory agencies. There are three types of institutions in the m-payment ecosystem that are covered by the new framework for PIs: i) money remitters; ii) MNOs; and iii) full range Payment Service Providers, e.g., credit card schemes. Payment Institutions are allowed to engage in three principal activities: i) foreign exchange services; ii) trustee of deposited funds; and iii) payment systems operations (Payment Services Directive, 2007).

Banks have traditionally served as the gatekeepers to the payment settlement system. Today, in many instances, nonbanks are now managing the networks and infrastructure used to process and settle transactions (Weiner, Bardford, Hayashi, Sullivan, Wang, & Rosati, 2007). Currently nonbanks play the largest role in processing card-based transactions, but their prevalence in the market for retail payments is expected to grow as e-commerce and m-payment channels develop. The growing importance of instruments like m-payments–which are characterized by a highly automated pre-transaction phase, online transaction processing, and real-time payment authorization–will create a more complex payment processing chain. Banks and nonbanks will need to coordinate their operations at numerous points of contact along this processing chain. Sensitive personal data will be communicated. The processing of transactions will only be as secure as its weakest link. Observers warn that banks may be exposed to new risks. They could be liable for payment fraud, even if the compromised data used to commit the fraud is acquired from a point in the transaction chain controlled by a nonbank (Weiner et al., 2007).

The growing role of nonbanks in the dominant four-party settlement system could also expose banks to new types of risks (Weiner et al., 2007). Banks are subject to strict regulations. They have proven successful at minimizing operational risks, preventing fraud, counterfeiting, and data breaches. Weiner and colleagues observed that it might not be desirable to subject nonbanks to a similarly stringent regulatory regime, which might reduce the economic incentives driving competition and innovation in electronic retail payments Nonbanks have technology and operational expertise that can enhances security (Weiner et al., 2007). The Directive creates broad authorization for PIs for three reasons. Regulators want to balance the need to expand the participation of nonbanks, to create more effective communication between banks and nonbanks, as well as to enhance the prudential management of nonbanks.

The second main object of the Directive is to simplify the rules concerning the rights and obligations of the users and providers of payment services (EUbusiness, 2007). The Directive aims to create a balance between the liability of merchants and consumers. Guidelines on the user's right to reject fraudulent

payments are introduced. The terms, conditions, and the appropriate timeline for the payment service provider to refund the user are outlined. For instance, the “full amount principle” defines the extent of consumers’ entitlement to be immediately reimbursed for the full amount in the event of an unauthorized electronic transaction if the user notifies their payment service provider about the fraud within 13 months (OECD, 2012). The Directive also introduces principles of transparency which mandate, for example, that transaction fees applied by the payment service provider must be listed separately, clearly stated, and not built into the price of the goods and services purchased. Payment service providers must also provide or make available a monthly statement of the consumers’ transactions. Another important measure is the Directive’s “D+1” provision, which states that all payment transactions are to be settled and executed no later than the next business day. While hours of operation can vary, payment service providers are required to state clearly in their contracts what time payment orders need to be received by in order for the payee’s bank to be credited on the next day business day (Turing, 2011).

4. South Korea and Japan

4.1. Introduction

In terms of rates of consumer adoption and the volume of transactions, South Korea and Japan are the global frontrunners in m-payment technology (Dapp, Stobbe, & Wruuk, 2012; KPMG International, 2007; OECD, 2012). Money moving through the m-payment channel in Japan had grown to make up 11.5 percent of the total volume of electronic money traffic by March 2009. In Japan, "e-money" banks are authorized to issue "electronic money," which is the equivalent of cash but stored on "smart cards," electronic devices or remote servers. The volume of transactions conducted with electronic money is growing rapidly. It surpassed debit cards in 2008 and reached 2 trillion (JPY) in 2011. Sales of the NFC-enabled mobile devices required for contactless m-payments reached 64 million units in Japan by 2009 (OECD, 2012). As of the end of August 2010, the largest platform for m-payments in Japan – the mobile network operator NTT Docomo's "iD" brand – claimed to have over 15 million subscribers (NTT Docomo, 2010).

South Korea has consistently led the world in the adoption of digital technology. The entire Asia Pacific region has been keenly observing the development of m-payments in South Korea, where electronic money is rapidly replacing cash as the dominant medium for retail transactions. More than 22.8 trillion won (KRW) changed hands electronically in 2008 (KPMG International, 2007)[7]. By 2009 more than four million people were using their mobile device every month to purchase transit passes, newspaper subscriptions, gym memberships, music, video games, and convenience store fare, for a total monthly volume of I.7 trillion (KRW) or $1.4 billion (USD). However, less than 1 percent of the total volume of electronic money transactions was exchanged with mobile devices in 2009 (Sang-Hun, 2009). The m-payment channels in South Korea and Japan are highly advanced relative to the rest of the world. Regulatory agencies are still taking a cautious approach to drafting new rules for m-payments. The focus is on encouraging new market entries, innovation, and enabling the growth of m-payments.

The position of regulators in Japan and South Korea is similar to that of their counterparts in the US and the EU. Adoption rates and transaction volumes are stronger in the former two countries, but m-payments are still thought to be in the early stages of development. Regulators appear to want to avoid hindering its development with premature regulation. Instead, the Korean Communications Commission has recently brought payment gateway service providers[8], MNOs, mobile device manufacturers, card networks and point-of-sale terminal manufacturers together to create an industry stakeholder consortium called the Grand NFC Korea Alliance. The Alliance works toward common goals, such as

[7] Industry observers predict that sales of NFC-enabled mobile devices in South Korea will reach 20 million in 2012. This would be the largest single rollout of mobile devices in the world with interoperable (i.e. non-proprietary) technology for contactless point-of-sale m-payments (Balaban, 2012).While Japan has more NFC-enabled mobile devices in the market (60 million), all of these units support "FeliCa" which is a proprietary technology of Sony Corp. and not interoperable with standard NFC mobile devices or readers (Balaban, 2012).

[8] Payment gateway service providers, or payment gateways, provide e-commerce and m-payment applications that authorize payments for merchants. Payment gateways encrypt sensitive data (e.g., credit card credentials) to allow information to be securely passed from the consumer to the merchant and payment processor.

growing the adoption rates of NFC-enabled devices, expanding the number of point-of-sale terminals for NFC-based transactions, as well as increasing m-payment interoperability (Balaban, 2012). The composition and goals of the Grand NFC Korea Alliance are similar to the Mobile Payment Industry Workgroup (MPIW) in the US and the SEPA initiative in the EU.

4.2. M-payments and the under-banked

The development of m-payments in Japan and South Korea was shaped to an important extent by the needs of the under-banked. Market research in the US has also found that young persons (18-24) and the under-banked population are more likely to be among the early adopters of m-payment technology. There is considerable overlap between these two segments of the population (Braunstein, 29 March 2012). However, different economic conditions tend to create under-banked populations with unique characteristics. Industry then adapts and responds to their needs in different ways based on the framework of regulation (Board of Governors of the Federal Reserve System, March 2012). The regulation and economic histories of Japan and South Korea have created unique gaps in the provision of financial services. The most successful m-payment businesses have evolved to serve the needs of under-banked consumers first.

In the research literature, two factors are recognized for shaping the development of the m-payments in Japan. First, large private banks traditionally played an important role in the functioning of the "keiretsu," which are the interlocking industrial enterprises that tended to dominate the Japanese economy in the second half of the twentieth century. Second, the government placed strict limits on the provision of short-term credit to consumers by banks in an effort to encourage household saving. At the core of each of the "big six" keiretsu are large private banks. While the dominance of the keiretsu has begun to decline, approximately one-half of personal financial assets in Japan are still held in bank deposits, the overwhelming majority of individuals have their salaries deposited directly into their bank accounts, and most have their bills withdrawn automatically from these same personal accounts (Dapp, Stobbe, & Wruuck, 2012). In other words, large private banks sit at the heart of Japan's economy and settlement system. It would have been logical to assume that those banks were well-positioned to become the central node between the various businesses that have converged in the m-payment market. According to observers, however, the strict limits on the provision of revolving credit by banks prevented them from playing a central role in the m-payment ecosystem. In essence, credit cards in Japan function like debit cards in North America. A closer analogue might be charge cards. The balance of a "credit card" is automatically deducted from a consumer's bank account at the end of each month. This has tended to mean that consumers in need of short-term credit were under-banked, or at least underserved by accredited financial institutions. This can push credit-worthy consumers into black market and even to loan sharks (KPMG International, 2007). This acute shortage of safe, convenient, and legal short-term credit was one of the main factors behind the rise of m-payments. When the government began easing restrictions on revolving credit, new financial institutions emerged to meet consumer demand with electronic money.

Seven companies dominate the electronic money market in Japan: Waon, Nanaco, Rakuten Edy, Suica, Pasmo, ICOCA and iD (Dapp, Stobbe, & Wruuck, 2012). These e-money banks are generally owned by

private railways, retailers, supermarkets, and shopping mall operators. E-money banks issue "smart cards," debit and credit cards to consumers. Contactless m-payments are made almost exclusively with "smart cards," as most credit cards are not contactless and no bank-issued debit cards are. MNOs usually include a function that allows "smart cards" to operate on mobile devices. NTT Docomo is the largest MNO in Japan. Their "iD" brand smart card is backed by the iD e-money bank. It is the largest m-payment platform by a wide margin, with a virtual monopoly on the Japanese m-payment market. NTT Docomo collects a rental fee for the use of its iD m-payment platform from the e-money banks that issue the smart card. They take a share of the merchant's transaction fees. They also charge merchants a rental fee on the smart card readers (i.e., terminals). Virtually all of the NFC-enabled mobile devices in Japan use FeliCa, which is proprietary technology of the Sony Corporation (Balaban, 2012). The average payment on a smart card is approximately 800 (JPY) or $10 (USD), so it does not compete with bank issued credit cards or money transfer services. Nevertheless, m-payments have already surpassed debit transactions and are rapidly replacing cash as the preferred method for making relatively small everyday retail transactions at supermarkets, restaurants, convenience stores, and public transit terminals (Dapp, Stobbe, & Wruuck, 2012).

Japan is unique to the extent that virtually all m-payments are provided through one business model: e-money bank issued "smart cards" for small denomination retail transactions on MNO provided m-payment platforms (KPMG International, 2007). As a result, experts describe the regulatory framework in Japan as quite straightforward. M-payments fall under the supervisory authority of the Ministry of Economy, Trade and Industry. NTT Docomo's iD m-payment platform is regulated as a consumer loan. Limits are imposed on the total amount that can be extended to individual consumers. There are also limits imposed on the rate of interest that can be charged on revolving credit extended through the m-payment channel.

The development of m-payments has been different in South Korea. Early initiatives between MNOs and banks in the 1990s and early 2000s were less successful. Private Banks tend to play a less central role in the economy. Observers report that competition and mistrust destabilized early partnerships between financial institutions and MNOs. Instead, third-party "payment gateway service providers" or "mobile PG service providers" (e.g., Danal, Mobilans, Infohub and Inicis) have been the primary developers of the m-payment channel (KPMG International, 2007). In South Korea, the under-banked segment of the population provided the initial demand for m-payments. Young people needed a cashless way to make payments for music and video content, computer games, software applications, etc. Payment gateways generally work by allowing consumers to "top-up" or deposit funds onto a prepaid card, which is then entered into the individual`s mobile device (KPMG International, 2007).

The m-payment market in South Korea is competitive. Seoul's municipal government, LG CNS, and the Korean Credit Card Union have launched the T-Money smart card for use on public transit systems, adjacent vending machines and convenience stores, as well as in the city's taxi fleet. More widely, MNOs like SKT and KT Freetel have teamed up with credit card networks to provide an alternative m-payment channel. For example, SKT and Visa have launched an m-payment service called SKT Moneta. In both the gateway and the MNO-credit card network business models, revenues are earned through service charges on transactions. In the case of MNO-credit card network services like SKT Moneta, charges of 3.5 percent

are assessed on each transaction. The transaction fees to use mobile PG service providers like Danal are considerably higher with the gateway assessing a charge of 3 percent and the MNOs taking a further 5 percent per transaction. Despite this disparity, gateways are competing head-to-head with SKT Moneta and KT Freetel's MasterCard-based m-payment service. However, gateways continue to target and cater to younger segments of the population who are under-banked and under-served by traditional financial institutions and credit card networks (KPMG International, 2007). Unlike Japan, the South Korean m-payment market is more diverse and its regulatory framework is worth considering in greater detail since the object of regulation is likely closer to the complex m-payment system evolving in North America and the EU.

4.3. South Korea's m-payment regulatory framework

Two pieces of legislation regulate m-payments in South Korea. The first version of the E-commerce Consumer Protection Act (ECPA) received assent in 2002. It underwent extensive revision in 2005 and the new Act took effect on 1 April 2006 (Blythe, 2006). The ECPA was written in response to a period of particularly high credit card fraud in the wake of the 1997 Asia economic crisis (KPMG International, 2007). In the decade after the crisis, supervisors developed a national strategy for promoting e-commerce by providing more clarity for industry on consumer protection rules. There are three obligations relevant to m-payments in the ECPA. First, consumers must be provided with complete information about the seller/merchant and, if applicable, the third-party payment service provider. This information should be available on the merchant's website. The consumer must also be provided with full details about dispute resolution procedures. Second, the merchant or third-party payment service provider has to provide the consumer with "use order forms" which give the consumer detailed information about their purchase and allow them to either confirm their purchases or make changes before it is authorized. Third, information disclosed by the consumer during the transaction must be protected by both the merchant and the payment service provider (OECD, 2012).

The Electronic Financial Transactions Act (EFTA) was passed in 2007. One of the more notable features of the EFTA is the way it makes financial institutions ultimately responsible for redress when consumers suffer losses as a result of fraud, unauthorized transactions, forgery, unfulfilled orders, etc. In essence, the EFTA holds the financial institution providing the settlement system responsible for resolving problems created downstream by MNOs, TSMs, payment gateways, third-party payment providers, merchants and sellers. Experience has taught South Korean legislators that it is very difficult for consumers to prove the nature of the liability, intent or negligence in the m-payment channel. It is highly complex. Transactions are instantaneous, and often automatic. The m-payment channel is also remote. Regulators have decided that it is better to hold the financial institution ultimately responsible to compensate consumers for their losses. Financial institutions can then use their expertise and resources to pursue the guilty stakeholder and exact the necessary compensation according to the terms of the contract. The EFTA holds this arrangement up as the best case scenario, however, "electronic financial business operators" (e.g., MNOs, gateways, credit card networks) will be held responsible for compensating consumers and pursuing other stakeholders when accredited financial institutions are not involved (Chung, 2012). Finally, any claim made by the consumer to secondary or third-party payment service providers must be

considered notification to the financial institutions and electronic financial business operators. Consumers are not expected to know that the financial institution is the ultimate reference point. The legal burden is on financial institutions to create effective lines of communication with their business partners.

Second, to ensure that m-payments are processed safely and reliably, the EFTA places financial institutions, electronic financial business operators, subsidiaries and third-party contractors, under the supervision of the Financial Services Commission (FSC).The FSC examines firms to make sure that they meet the standards for safe and secure processing of m-payments and e-commerce set out in the EFTA (e.g., information technology, manpower, facilities, and electronic equipment) (Chung, 2012). Industry stakeholders are also required to submit performance reports to the FSC.

Third, the EFTA also requires financial institutions and electronic financial operators to create and securely maintain detailed records of all m-payment and e-commerce transactions for a period of not less than five years. These records must also be made available to stakeholders, regulators and consumers for the purposes of investigations, to verify their accuracy, as well as to trace and rectify errors or instances of fraud (Chung, 2012).

Fourth, with respect to privacy and disclosure, the EFTA requires all industry stakeholders to receive the informed consent of consumers before disclosing personal information related to the identity of the individual, or details concerning the individual's transactions and accounts, to third-parties that are not directly involved in the transaction that produced the data. Furthermore, stakeholders that are directly involved in the transaction must receive the informed consent of consumers before using the data towards any purpose not directly related to processing the original transaction (Chung, 2012).

Finally, the EFTA requires financial institutions and electronic financial operators to keep separate accounts for each financial business in order to facilitate more effective regulatory audits. Prudential requirements are also specified in the legislation (e.g., the ratios of bank deposits to the credit extended by payment gateways to consumers who are not obligated to settle accounts immediately). The Korean Fair Trade Commission (KFTC) has given municipal and provincial governments the power to supervise third-party payment service providers and to make sure that they do not abuse their position in an anticompetitive manner. The Telecommunications Business Act requires the operators of online marketplaces to acquire a "value added service provider" license and to file reports to the Ministry of Information and Communication (KPMG International, 2007).

5. Kenya and the Developing World

5.1. Under-developed financial systems and highly developed mobile money networks

Unlike the developed world, where m-payments allow consumers to access existing payment sources via new technology, m-payments are playing an important role in the transformation of financial products and services across the developing world. “Mobile money” is the term used for electronic money in most developing countries. Mobile money is now available to consumers for the purposes of conducting transactions through their mobile devices; it is electronically recorded; and can be redeemed for cash as well (Castri, 2013). Mobile money encompasses a wide range of other services as well, such as m-payments, mobile finance (e.g., insurance products), and mobile banking (Klein & Mayer, 2011; Ndiwalana & Popov, 2008; World Bank, 2012).

There are two models of mobile financial services in developing economies. First, there is a bank-based model in which the consumer has a direct contractual relationship with a licensed and supervised financial institution. In some cases consumers have an account with the financial institution. In other instances, the consumer uses a financial institution to make one transaction. Afterwards the consumer can deal exclusively with a retail agent who handles any further communication with the financial institution (Sultana, 2009). Generally, the bank-led model is seen as a way for established financial institutions to provide new services to existing customers (Lachaal & Zhang, 2012).

The second model is the MNO-led model. This model has experienced faster growth. It is credited with playing a transformational role because it is providing unbanked or under-banked populations with access to financial services for (Klein & Mayer, 2011; Lachaal & Zhang, 2012; Sultana, 2009). Kenya’s M-PESA is one of the most successful mobile money brands in the world. Safaricom is Kenya’s largest MNO with a market share of approximately 80 percent (Jack & Suri, 2011). In 2007, Safaricom launched M-PESA to serve urban Kenyans who wanted to send money home to relatives in rural areas. This form of urban-to-rural remittance had been difficult because it was underserved by financial institutions (Veniard & Goss, 2012). In essence, Safaricom extended a practice that was already commonplace. Most MNOs allowed individuals to purchase pre-paid cell phone credit. Safaricom enabled consumers to send this credit to other users through SMS texts. Consumers could then “on-sell” it to a local agent in return for cash or goods and services (Jack & Suri, 2011). According to Jack and Suri (2011), M-PESA functions in the following manner: Registered customers make deposits (known as “e-floats”) with M-PESA agents using their mobile device and a Safaricom SIM card. M-PESA operates and manages consumers’ accounts and allows consumers to carry an e-float balance. A fee is assessed for withdrawing funds, but there are no charges on deposits. An e-float can be transferred to another person via SMS text message for a nominal flat-rate fee. No fee is assessed on the receiver of the funds until a withdrawal is made. M-PESA agents hold e-float balances on their mobile devices and are required to maintain a certain amount of cash on site. The balances are then either purchased from Safaricom or other customers through agents (Jack & Suri, 2011). M-PESA began as a remittance service. It has quickly evolved into a vehicle used for a wide

range of payments. In April 2011, Safaricom reported that there were 14 million M-PESA customers and nearly 28,000 agent outlets (Safaricom, 2011).

M-PESA is widely seen as a model that should be emulated in other countries in the developing world (Jack & Suri, 2011; Lachaal & Zhang, 2012). Similar to the recent history of m-payments in South Korea, it has been under-banked and unbanked consumers in Kenya who have tended to adopt mobile money first. There are approximately 40 million people in Kenya. Most of the population lives in rural areas where financial services are scarce. Only 4.23 percent of adults have an account at a financial institution (World Bank, 2012). However, the rate of mobile device penetration is over 75 percent (iHub Research; Research Solutions Africa, 2012). Across the developing world people are more likely to have access to mobile phone networks than basic financial services. The proportion of individuals over the age of 15 that have a debit card is 34.5 percent in the East Asia and Pacific region, 9.1 percent in the Middle East, and 7.2 percent in North Africa (World Bank, 2012). However, there are nearly 5 billion mobile phone subscriptions in developing countries, representing approximately 83 percent of all mobile subscriptions in the world (World Bank, 2012). As a result of M-PESA's success, there has been a proliferation of mobile money offerings across the developing world.

The advent of mobile money can be seen as a remedy for financial exclusion. Communities are gaining access to financial services through a virtual and mobile infrastructure with mechanisms that often supersede financial institutions (Klein & Mayer, 2011). The proliferation of mobile money solutions in developing economies demonstrates a large demand for banking services and payment alternatives. Coupled with the prevalence of mobile devices and consumers' willingness to adopt mobile applications, mobile financial services are ultimately being used to promote financial inclusion and drive economic development (di Castri S. , 2013; Klein & Mayer, 2011; Swedish International Development Cooperation Agency, 2010; World Bank, 2012).

5.2. Prudential regulation

At this time, the structural soundness of mobile money operators appears to be the main concern for regulators. The mobile money ecosystem is complex and comprised of various parties, stakeholders, multiple contracts and service arrangements. Observers note that supervising mobile financial transactions requires cooperation and coordination across different structures of governance (e.g., regulators and policymakers), industry representatives (e.g., mobile network operators, financial institutions, retail agents, third party content service providers, equipment manufacturers), and end-users (Klein & Mayer, 2011; Ndiwalana & Popov, 2008). As a result, regulators from various sectors tend to address overlapping issues.

The rise of MNOs operating like financial institutions has led regulators to focus their initial efforts on the prudential regulation of non-banks. As Klein and Mayer (2011) have noted, "Policymakers and regulators in countries ranging from Namibia to Indonesia, from Mexico to the Philippines and from Kenya to Pakistan are drafting regulations for the era of mobile money. They struggle with adapting banking regulation to mobile banking." New prudential requirements are designed to maintain the integrity of the

institution's capital and a certain level of liquidity. These requirements include minimum capital ratios, capital adequacy measurement systems, and reserve requirements (Castri, 2013). For instance, in the case of Kenya's M-PESA service, Safaricom does not use deposits to extend credit. Safaricom functions as a collector of deposits that "stores and transfers money" (Klein & Mayer, 2011). The agents who exchange book-entry money are free-standing businesses that do not put the consumer's money at risk through investments (Klein & Mayer, 2011). As such, it is difficult to apply existing prudential regulation to services that are unconventional and do not replicate the services of regulated financial institutions.

One approach being adopted is the concept of functional decomposition, which is a form of regulation based on the services or products offered by firms rather than the type of institution the firm is. Functional decomposition requires supervisory agents to ask what form of regulation is appropriate for each type of service (Klein & Mayer, 2011). The mobile money system has highlighted the distinction between "different components of financial services… [and functional decomposition] helps to establish where the focus of regulation should lie" (Klein & Mayer, 2011). This approach also helps to clarify whether the provision of mobile financial services modifies or adds to the risks consumers typically face when they use traditional channels (Sotomayor, 2012). Regulators assess the potential risks and anticipated benefits introduced by each type of institution, activity, product, or service, and design supervision so that the regulatory burden is proportionate (Lauer, Dias, & Tarazi, 2011).

In the absence of established prudential rules, regulators and the firms deploying mobile money are continuously implementing new solutions to try and keep pace with the rapidly evolving financial system and telecommunications industry. For M-PESA, the Central Bank of Kenya requires the service provider to invest the net deposits from customers' transactions in regulated banks for security and safe-keeping. In the Philippines, where the regulatory environment is reportedly flexible and accommodating to innovation, Globe Telecommunications created a subsidiary company, G-Xchange, to manage the financial aspects of their mobile money application "G-Cash." This subsidiary is then regulated by the Central Bank of Philippines (Ndiwalana & Popov, 2008). The Central Bank of Philippines also established the Core Information Technology Supervisory Group to increase their capacity to regulate the mobile money environment (Ndiwalana & Popov, 2008).

Overall, there appears to be a need for greater coordination between stakeholders (Ndiwalana & Popov, 2008). Observers are urging regulators to review national policy and the legal environment, to build capacity, and to encourage collaboration between supervisory agencies and the private sector (Kimenyi & Ndung'u, 2009; Ndiwalana & Popov, 2008). Policymakers are endeavouring to construct a flexible regulatory framework that will "create an open and level playing field that fosters competition and innovation, leverages the value proposition of both banks and non-bank providers, attracts investment, and allows providers to focus on refining operations and promoting consumer adoption" (di Castri S. , 2013; Ndiwalana & Popov, 2008). In addition, mobile money firms are navigating the regulatory requirements of various sectors to ensure that their services are fully compliant.

5.3. Regulatory frameworks and consumer protection

The concerns and risks for consumers using mobile money are similar across the developing world. However, there are some important differences which stem from unique economic conditions. Many jurisdictions have only recently adopted financial consumer protection frameworks. Few have regulations relevant to mobile money or MNO-led mobile money offerings. Recently, when the Consultative Group to Assist the Poor (CGAP) analyzed financial consumer protection in the Europe/Central Asia region (i.e., Albania, Armenia, Azerbaijan, Bosnia, Georgia, Kazakhstan, Kosovo, Kyrgyz Republic, Macedonia, Russia, Serbia, and Tajikistan), they found that most did not begin to develop rules until 2008 (Consultative Group to Assist the Poor, 2012). These regulations typically address "fundamental consumer protection principles such as transparency and disclosure, fair treatment, and recourse mechanisms" for banking products such as loans and deposits (Consultative Group to Assist the Poor, 2012). However, since the regulations tend not to apply to non-bank financial service providers, consumer protection varies depending on the source of funds used to make the payment. The following discussion provides synopses of existing regulatory approaches and consumer protection measures in Kenya, Bangladesh, and India.

5.3.1. Kenya

M-PESA was launched in March of 2007 in Kenya, a jurisdiction that had no laws, regulations, or policies that were directly applicable to electronic money transactions (Sultana, 2009). As a result, mobile financial services evolved quickly in a largely undefined regulatory space (Flaming, et al., 2011). To ensure adherence to standard banking practices, Safaricom consulted the Central Bank of Kenya in August 2006. Since then the Central Bank has continued to provide oversight and guidance (Flaming, et al., 2011). Through collaboration and innovation, the Central Bank and Safaricom have addressed emerging challenges vis-à-vis the introduction of new mobile money services as well as consumer protection initiatives (Flaming, et al., 2011). For example, after a thorough review of its practices, the Central Bank concluded that M-PESA was not a banking business as defined by the Banking Act given that "cash exchanged for electronic value are not repaid on terms … or lent in the pursuit of other business or interest income" (Sultana, 2009). Safaricom was then asked to complete and submit a detailed risk mitigation strategy and once it was approved they were permitted to implement M-PESA shortly thereafter (Sultana, 2009). Safaricom also developed its own approach to disclosure, fair conduct and dispute resolution, with specific but informal guidance from the Central Bank (Flaming, et al., 2011). Likely as a result of this effective working relationship between Safaricom and the Central Bank, M-PESA emerged with consumer-friendly policies in spite of the absence of consumer protection laws (Dias & McKee, 2010).

Since the implementation of M-PESA, the Central Bank of Kenya has made some changes to the regulatory framework for mobile financial services. In 2010, the Central Bank enacted *Guidelines on Agent Banking* to prescribe the manner in which agents (e.g., mobile money agents) should conduct business in Kenya so that the supervision, safety and soundness of the banking sector is ensured (Boston University, 2013; Central Bank of Kenya, 2010). In 2011, the Bank enacted the *National Payment System Act* to supervise payment systems and to more clearly articulate which firms will be defined as payment service providers and regulated accordingly (Central Bank of Kenya, 2011). Through the *National Payment System Act*, a broader regulatory and consumer protection framework for the mobile financial services industry is now beginning to unfold in Kenya.

5.3.2. Bangladesh

There are five active mobile money services firms in Bangladesh. The Bangladesh (Central) Bank has implemented measures to regulate electronic payment services and protect consumers. In 2009, the Bank enacted the Payment and Settlement Systems Regulations to formalize their authority to grant licenses for payment systems, payment system operators and payment service providers (Sultana, 2009). As a result, the Central Bank has the power to classify new financial services and products (e.g., electronic money) as a designated payment instrument (Sultana, 2009). Once the Central Bank has defined these services as payment instruments, the firms providing these services are obliged to follow a series of applicable guidelines.

In an effort to mitigate the risks posed by cross-sectoral partnerships involving banks, only entities that are authorized by the Central Bank can issue electronic money. The regulations do exempt existing banks and financial institutions from acquiring a license. Before authorized account providers can enter into customer service agreements, they must practice due diligence through a "know your customer" process. To monitor the money supply and protect customers by ensuring the integrity, security and reliability of the payment system, account providers must also adhere to the 2002 *Money Laundering Prevention Act* and prohibit cross border money transfers (Sultana, 2009; Klein & Mayer, 2011).

5.3.3. India

In an effort to mitigate the challenges associated with monitoring new mobile financial service providers, the Reserve Bank of India issued *Operative Guidelines for Banks* in 2008. They address the implementation of new currency control regulations. According to the *Guidelines*, only banks that are licensed, supervised and physically present in India are permitted to offer mobile financial services to residents (Reserve Bank of India, 2009). Non-banks are now prohibited from issuing electronic money. The Guidelines require that "services should be restricted to bank accounts and/or credit card accounts in India which are [know your customer/anti-money laundering] compliant." Furthermore, it states that only Indian rupee-based services (i.e., services using Indian currency) should be provided (Reserve Bank of India, 2009). Cross-border money transfers are, therefore, strictly prohibited under the new regulations. Account providers must also adhere to the 2002 *Prevention of Money Laundering Act* and the 1986 *Consumer Protection Act*.

6. Conclusion

6.1. The United States

Our US review considered expert opinion on the regulatory issues associated with the growth of m-payments. To summarize these opinions, the emergence of m-payments has created challenges for the relatively complex framework of regulation in the US. The m-payment market involves a large number of firms from different industries. There is a pressing need to clarify the responsibilities of each agency for the different aspects of this new payment channel. There may not necessarily be a need for new regulation. However, complexity can create ambiguity over supervisory authority. Complexity can also allow for the emergence of gaps in the consumer protection framework.

Observers point to promising results that have been achieved because Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act (2010) has centralized rulemaking authority for federal consumer protection law within the CFPB. Before this transfer of authority in 2011, m-payments would have been under the authority of five financial regulators at the federal level. The centralization of supervisory authority for m-payments under the CFPB has greatly simplified the landscape. Reform has also created a single federal agency with a strong interest in reforming the framework, and the authority to enhance the protection of consumers, as financial products and services evolve.

There is some debate over which m-payment technologies should be open and shared and which can be closed or proprietary, as well as whether regulators should have a role in establishing the rules for interoperability. There is a general consensus that m-payment technology should be interoperable at the point-of-sale. This would help to facilitate the development of an m-payment system that can offer consumers a seamless experience on par with debit and credit card options.

However, there is little consensus over whether m-payments should be interoperable at higher levels, such as the establishment of common standards for secure element (SE) technology. The firm that controls the SE typically controls the valuable consumer data generated by m-payments. Regulators have to balance the need to safeguard the security of consumers' data with the need to offer economic incentives to the firms competing to develop m-payment technology.

The widely publicized dispute between Google and Verizon illustrates how security and interoperability are linked. Google took steps to strengthen the objective security of their Mobile Wallet. Nevertheless, because their cloud/SE hybrid design solution is proprietary, rival firms continue to press Google to provide further proof that their m-payment technology is adequately secure. Underlying these apparent concerns about the security of consumers' data, there are strong commercial interests in acquiring access to the new data produced by m-payments. The industry stakeholder that owns or controls the m-payment users' data gains the strategic advantage. The eventual resolution of the disagreement between Verizon and Google also illustrates the willingness of industry stakeholders to resolve disputes and create mutually beneficial commercial contracts without regulatory guidance.

For regulators charged with supervising consumer protection, the question might be whether these contracts sufficiently safeguard the rights and privacy of consumers. There are experts who argue that the struggle over interoperability is best resolved by existing anti-trust laws and the regulations governing intellectual property and competition (Brown, 2012). This position is further supported by the assumption that the complexity of the m-payment ecosystem makes one-size-fits-all solutions undesirable. Instead, it might be preferable to allow industry to negotiate contracts that stipulate the extent of interoperability, revenue sharing, ownership of consumer data, the responsibility to protect the security of users, and procedures of redress (Brown, 2012).

Contrary to this position, the MPIW has argued that regulators should broaden their mandate to either enforce specific rules or guide industry stakeholders towards interoperability at the level of SE design. Their solution is to hand the responsibility for SE management over to Trusted Service Managers or TSMs, which would oversee the production of SEs, the settlement of transactions, and the secure management of consumer data. Transferring responsibility for SE to TSMs would facilitate coordination between industry stakeholders by allowing data to be shared via commercial contracts with TSMs rather than monopolized through proprietary technology (Continie, Crowe, Merritt, Oliver, & Mott, 2011). Currently, the problem identified with this solution is the absence of TSMs that have resources and expertise that approach major internet players like Google. What appears to be happening instead is that MNOs are forming joint ventures to create TSMs, while Google remains resolute in its intention to manage consumer data over its own internet servers (e.g., the cloud/SE hybrid design in the most recent Google Wallet platform).

Finally, the literature indicates that there are gaps in the regulatory framework for protecting consumers' privacy in the US, both in the sense of protecting consumers' data but also in the broader sense of protecting consumers' autonomy. The m-payment ecosystem will likely be predicated on harvesting consumer data, generating highly individualized consumer profiles, and then reaching consumers with new forms of direct and targeted marketing. The present framework is reportedly insufficient to allow consumers to be informed about, or to choose to opt-out of, behavioural targeted advertising. Current regulations are also criticized for not empowering consumers to use the profiles generated about them to make informed choices in response to this type of marketing. Any attempt to reform the existing framework or to draft new regulation must first take account of the complexity of the existing landscape. The complexity of the framework means that new guidelines could hamper the development of the m-payments or work at cross-purposes with regulation overseen by other agencies (e.g., new regulation to protect consumer privacy could contradict disclosures required to supervise banking transactions for illegal activity).

6.2. The European Union

The primary issue for policymakers in the EU is harmonization. Experts observe that businesses and people currently cross national political boundaries in the EU with much greater ease than retail payments. The European Commission views m-payments as a vehicle for furthering the realization of a seamless single market across the EU member states. Results have been mixed.

Some have contended that regulatory fragmentation has hindered the European Payment Council's (EPC) goal of achieving a seamless "single market" for retail payments across member states. The EPC and the European Central Bank (ECB) anticipate that the growth of m-payments will help to steer industry stakeholders and national regulatory agencies towards compliance with SEPA's frameworks. However, consumers and merchants are not going to adopt m-payments in large numbers until the experience is more convenient, secure and efficient than the payment options that already exist. Presently, regulators are faced with a chicken-and-egg problem: development of the m-payment system requires further harmonization of the regulatory framework and development of the m-payment channel is needed to motivate industry to comply with harmonized regulation.

The debate between stakeholders over transaction fees illustrates the multiple challenges associated with the EU's use of voluntary instruments to govern the m-payment ecosystem. Interchange fees have become a concern for regulators because charges vary significantly between national jurisdictions and additional surcharges are levied on transactions settled between issuing and acquiring banks that originate in different national jurisdictions. Interchange fees are seen as a barrier to harmonization.

There is some debate over whether interchange fees are also a consumer protection issue. Industry experts have argued that transaction fees are rising despite strong competition. Issuing banks attract cardholders with more generous reward programs, which are funded by higher interchange fees. Acquiring banks pay interchange fees with revenue earned from merchant service charges. Merchants increase retail prices for all consumers, regardless of their method of payment, to cover expenses related to merchant service charges. Presently, consumers cannot avoid higher retail prices by choosing to pay with cash or debit. Consumers who pay with cash are subsidizing the cost of the transactions conducted by consumers who hold premium credit cards. Cross-subsidies are widespread in modern economies, but payment systems play a central role in facilitating commerce. The recent decision by the EU to regulate interchange fees could influence the way transaction fees evolve in the m-payment ecosystem.

The EU's Data Protection Directive is one of the most advanced regulatory frameworks of its kind in the world. The eight core principles have been lauded and, in general, the Directive is praised as a positive step towards more adequate protection of consumers' data, as they engage in e-commerce and conduct m-payments (Robinson, Graux, Botterman, & Valeri, 2009). Strengths include the technology-neutral language and definitions as well as the flexible and adaptive principles-based framework of rules. The Directive offers an effective way to balance an individual's willingness to be persuaded to divulge personal data when it is in their interests with assurances that the harvesting and processing of this personal data will be lawful and fair. The Directive could still eventually become inadequate, given the rapid evolution of e-commerce and m-payment channels.

One of the problems identified with the framework is its uneven adoption, adaptation and enforcement across national jurisdictions. For example, Bygrave (2000) observes that the definition of "sensitive" data covered under principle eight varies significantly in different domestic adoptions of the Directive; most jurisdictions define race and ethnic origins, political opinions, sexual orientation and health information, as "sensitive" but definitions of group membership, associations and trade unions vary, as do protections offered to data concerning the receipt of social welfare benefits. Robinson and colleagues note that,

because the harvesting and processing of personal data is global, the Directive's approach to supervising data will also need work across international boundaries (Robinson et al., 2009). While compatible regulations have been adopted in 39 jurisdictions outside Europe to go along with the 50 countries that have adopted the Directive within Europe, the US and China are tremendously important trading partners and both have abstained thus far (Greenleaf, 2012). Greenleaf (2012) argues that the importance of China and the US cannot be overstated. Measures are needed to harmonize regulations between these two political entities and the EU. Another key weakness is the simplistic and static definition of the "data controllers" that gather and process consumers' data (Robinson et al., 2009).

King and Jessen (2010) have observed that the most important regulatory gaps with respect to the m-payment channel might be the ambiguity surrounding the Directive's definition of personally identifiable information (PII). The Directive largely confines its scope to PII, which has had the unintended consequence of creating a strong economic incentive for data controllers to define the data they gather and process as "anonymous" or "non-PII" to avoid regulation. For instance, there is ambiguity over whether "secondary identifiers" like Internet Protocol (IP) addresses and "HTTP cookies" should constitute PII. "Dynamic" IP addresses, which change over time with each session as mobile device users log on and off the internet and MNO networks, and "HTTP cookies", which are small pieces of data that are automatically downloaded from websites and stored on web browsers, are both used by data harvesters and processers to track mobile device user's online activity and to generate consumer profiles. The status of these profiles as either PII or anonymous data is unclear, which means that the status of the consumers' rights pertaining to participation and control, informed consent, and third party-disclosure, as outlined in the Directive, are also uncertain.

King and Jesson (2010) argue that clearer rules might be needed to ensure that secondary identifiers and PII cannot be linked when the former are classified as non-PII. The EU has formed a working group to consider these gaps and their preliminary recommendation is to enforce a kind of "precautionary principle." This would mean that dynamic IP addresses will be considered PII unless data controllers can prove otherwise. This means that the assumption will be that dynamic IPs can be linked to PII or used to generate PII and, therefore, the burden will be on data controllers to prove the anonymity of their data to exempt it from the Directive (King & Jessen, 2010).

6.3. South Korea and Japan

There are two crucial lessons to observe from the experience of Japan and South Korea. First, the evolution of m-payments in these countries has been profoundly shaped by the needs of the under-banked, who tended to be the early adopters of the technology. Consumer access to short-term revolving credit was limited in Japan and m-payment providers were among the first firms to capitalize on liberalization. Young people with high rates of mobile device adoption but little access to credit and few ways to conduct electronic transactions were the first to subscribe to m-payment services in South Korea. This is important for supervisory agencies because it suggests that protecting consumers in the m-payment channel will require programs that can reach out to and improve the financial literacy of the under-banked.

Second, while regulators in South Korea are concerned not to stifle the evolution of m-payments by enacting regulations that are unduly burdensome, in 2007 legislators passed two relatively extensive and detailed frameworks to protect consumers in the m-payment channel (OECD, 2012). In a sense, South Korea demonstrates how regulation can serve to propel m-payments forward by creating greater certainty for industry.

The regulatory framework in South Korea is highly sophisticated and worth considering. Even though it is one of the most advanced regulatory frameworks of its kind, the E-commerce Consumer Protection Act (ECPA) was still deemed inadequate to supervise the host of new legal issues that emerged with the growth of mobile banking, e-commerce, and m-payments. One issue was its technology-neutral language (Chung, 2012). To address these gaps, legislators drafted and passed the Electronic Financial Transactions Act in 2007. The scope of EFTA is designed to broaden supervision to include third-party payment service providers (i.e., payment "gateways") as well as MNOs and financial institutions. It delineates their specific obligations to each other, consumers, and merchants. Critics have suggested that the EFTA may also prove inadequate as m-payments continue to grow and evolve.

6.4. Kenya and the Developing World

The growth of mobile money in developing countries has been dramatic. Innovative companies like Safaricom have taken advantage of relatively high rates of mobile phone penetration to develop financial services and meet the needs of large numbers of unbanked and under-banked consumers. Following the considerable success of Safaricom's M-PESA in Kenya, MNO-led business models are now being adopted across the developing world. This is likely to continue for the foreseeable future given that mobile financial services can be used as a tool for financial inclusion and economic development. However, the fact that regulation and legislation has not kept pace with mobile money innovation is a concern (Ndiwalana & Popov, 2008). Observers are encouraging regulators, policymakers, service providers and other parties to continue to address risks, especially in the area of consumer protection. Furthermore, they suggest that there is a need for service providers to expand product offerings to meet emerging needs. Finally, regulators have been encouraged to provide consumer education tools and to inform consumers about the benefits and risks of mobile money.

7. Bibliography

About the European Payments Council (EPC). (2013). Retrieved March 2, 2013, from European Payments Council: http://www.europeanpaymentscouncil.eu/content.cfm?page=what_is_epc

Andrei, V., Rusu, S. M., Diaconescu, S., & Dinescu, A. (2011). Securing On-Line Payment Using Dynamic Signature. *Journal of System and Management Science , 1* (1).

Balaban, D. (2012, January 12). South Korea Takes Lead Globally in NFC Rollouts with Millions of Phones and SIMs. *NFC Times* .

Bergevin, P., & Zywicki, T. (2012). *Debit, Credit, and Cell: Making Canada a Leader in the Way We Pay.* Toronto: C.D. Howe Institute.

Black, J. (2008). Forms and paradoxes of principles-based regulation. *Capital Markets Law Journal , 3* (4), 425-457.

Blythe, S. E. (2006). The tiger on the Peninsula is digitized: Korean E-Commerce Law as a driving force in the world's most computer-savvy nation. *Houston Jounral of International Law , 28* (3).

Board of Governors of the Federal Reserve System. (March 2012). *Consumers and Mobile Financial Services.* Survey, Washington, DC.

Borestam, A., & Schmiedel. (2011). Interchange Fees in Card Payments. *European Central Bank: Ocassional Paper Series , 131*.

Boston University. (2013, March 2). *Boston University Center for Finance, Law & Policy*. Retrieved from Laws under Consumer Protection: http://www.bu.edu/bucflp/laws/by-type/consumer-protection/

Braunstein, S. F. (29 March 2012). *Statement to the Senate Hearing on Mobile Payments.* Committee on Banking, Housing, and Urban Affairs . Washington, DC: U.S. Senate.

Brown, T. P. (2012). *Statement to the Senate Hearing on Mobile Payments.* Committee on Banking, Housing, and Urban Affairs. Washington, DC: U.S. Senate.

Bureau of Consumer Financial Protection. (2012). *Docket No. CFPB-2012-0019 (Advanced Notice of Proposed Rulemaking, Regulation E, GPR cards).* Washington.

Bygrave, L. A. (2000). Core principles of data protection. *Privacy Law and Policy Reporter , 6* (8).

Canadian Bankers Association. (2012). *How Canadians Bank.* Toronto.

Canadian Payments Association. (2013). *Examining Canadian Payment Methods and Trends.* Ottawa.

Central Bank of Kenya. (2010). *Boston Center for Finance, Law & Policy.* Retrieved from Guideline on Agent Banking - CBK/PG/15: http://www.bu.edu/bucflp/files/2012/01/Guideline-on-Agent-Banking-CBKPG15.pdf

Central Bank of Kenya. (2011). *National Council for Law Reporting.* Retrieved from The National Payment System Act, 2011: http://www.centralbank.go.ke/images/docs/legislation/NATIONAL%20PAYMENT%20SYSTEM%20ACT%20(No%2039%20of%202011)%20(2).pdf

Charter of Fundamental Rights of the European Union, 2000/C 364/01 (European Convention December 7, 2000).

Children's Online Privacy Protection Act, 6501-6506 (Pub.L. 105-277, 112 Stat. 2581-728) (Federal Trade Commission October 21, 1998).

Chung, C. H. (2012). Liability Issues Arising from Mobile Finance. *Banking and Finance Law Review , 27* (2).

Cirasino, M., & Ratha, D. (2009). The Activities of the Global Remittaces Working Group. *G8 International Conference on Remittances* (pp. 1-22). Rome: World Bank.

Consultative Group to Assist the Poor. (2012). *Financial Consumer Protection Regulation in Europe/Central Asia.* CGAP.

Continie, D., Crowe, M., Merritt, C., Oliver, R., & Mott, S. (2011). *Mobile Payments in the United States: Mapping the Road Ahead.* Boston, MA: Federal Reserve Bank of Boston, Federal Reserve Bank of Atlanta, BetterBuyDesign.

Continie, D., Crowe, M., Merritt, C., Oliver, R., & Mott, S. (2011). *Mobile Payments in the United States: Mapping the Road Ahead.* Boston, MA: Federal Reserve Bank of Boston, Federal Reserve Bank of Atlanta, BetterBuyDesign.

Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, European Treaty Series No. 108 (Council of Europe January 28, 1981).

Crowe, M., Kepler, M., & Merritt, C. (2012). *The U.S. Regulatory Landscape for Mobile Payments: Summary Report of Meeting between Mobile Payments Industry Workgroup and Federal and State Regulators.* Boston, MA: Federal Reserve Bank of Boston and Federal Reserve Bank of Atlanta.

Crowe, M., Kepler, M., & Merritt, C. (2012). *The U.S. Regulatory Landscape for Mobile Payments: Summary Report of Meeting between Mobile Payments Industry Workgroup and Federal and State Regulators.* Boston, MA: Federal Reserve Bank of Boston and Federal Reserve Bank of Atlanta.

Cunningham, L. A. (2007). A Prescription to Retire the Rhetoric of "Principles-Based Systems" in Corporate Law, Securities Regulation and Accounting. *Boston College Law School Faculty Papers , Paper 195*.

Dapp, T. F., Stobbe, A., & Wruuck, P. (2012). *The future of (mobile) payments: New (online) players competing with banks.* Frankfurt am Main, Germany: Deutsche Bank Research.

Dapp, T. F., Stobbe, A., & Wruuck, P. (2012). *The future of (mobile) payments: New (online) players competing with banks.* Frankfurt am Main, Germany: Deutsche Bank Research.

di Castri, S. (2013). *Mobile money: Enabling regulatory solutions.* London: GSM Association.

di Castri, S. (2013). *Mobile Money: Enabling regulatory solutions.* London: GSM Association.

Dias, D., & McKee, K. (2010). Protecting Branchless Banking Consumers: Policy Objectives and Regulatory Options. *Focus Note* (64).

Directive on Privacy and Electronic Communications, 2002/58/EC (European Parliament and Council July 12, 2002).

Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 95/46/EC (European Parliament and Council November 23, 1995).

Electronic Fund Transfers Act (Regulation E), 12 CFR part 1005.76 FR 81019 (Bureau of Consumer Financial Protection December 30, 2011).

EUbusiness. (2007, April 24). *Payment Services Directive: Frequently Asked Questions*. Retrieved March 15, 2013, from Eubusiness: http://www.eubusiness.com/topics/finance/payment-services-qa/

European Central Bank. (2006). *Towards a Single Euro Payments Area: Objectives and Deadlines (4th Progress Report).* Frankfurt am Main: ECB.

European Commission. (2012a). *Feedback statement on European Commission Green Paper "Towards an integrated European market for card, internet and mobile payments".* Brussels: EC.

European Commission. (2012). *Green Paper: Towards an integrated European market for card, internet and mobile payments.* Brussels: EC.

European Commission. (2012). *Green Paper: Towards an integrated European market for card, internet and mobile payments.* Brussels: EC.

European Commission. (2012c). *Press Release: Antitrust: Commission welcomes General Court Judgment in MasterCard case (Ref: Memo/12/377).* Brussels: Europa.

European Commission. (2012b). *Press Release: Antitrust: Commsision sends supplementary statement of objections to Visa (Ref IP/12/871).* Brussels: Europa.

European Convention on Human Rights, Protocol No. 14 (European Court of Human Rights, Council of Europe June 1, 2010).

European Payments Council. (2012). *White Paper: Mobile Payments, Version 4.0 (EPC492-09) .* Brussels: EPC.

Evans, D. S. (2011). *Interchange Fees: The Economics and regulation of What Merchants Pay for Cards.* Comeptition Policy International.

Evans, D. S., & Mateus, A. (2011). *How Changes in Payment card Interchange Fees Affect Consumers Fees and Merchant Prices.* London: Social Sciences Research Network.

Fair and Accurate Credit Transactions Act, Pub.L. 108-159 (108th United States Congress November 22, 2003).

Fair Credit Reporting Act, Title VI, Pub.L. 91-508 (84 Stat. 1114) (91st United States Congress October 26, 1970).

Financial Services Modernization Act, Pub.L. 106-102, 113 Stat. 1338 (106th United States Congress November 12, 1999).

Flaming, M., Owino, A., McKee, K., Jentzsch, N., di Castri, S., Maina, B., et al. (2011). *Consumer Protection Diagnostic Study - Kenya.* Nairobi: Financial Sector Deepening Kenya.

Ghag, O., & Hegde, S. (2012). A comprehensive Study of Google Wallet as an NFC Application. *International Journal of Computer Applications , 58* (16), 37-42.

Google. (2013). *Google Wallet FAQ*. Retrieved February 23, 2013, from Google Wallet: http://www.google.ca/wallet/faq.html#general-in-store

Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108? *Edinburgh School of Law Research Paper Series* (pp. 1-36). Edinburgh: University of Edinburgh.

Haas, M. (2012). *Response to the European Commission - Consultation on Green Paper: Towards an integrated European Market for Card, Internet and Mobile Payments.* PayPal EU Liason Office.

Hayashi, F., & Weiner, S. (2005). *Competition and Credit and Debit Card Interchange Fees: A Cross-Country Analysis.* Federal Reserve Bank of Kansas City.

Health Insurance Portability and Accountability Act, Pub.L. 104-191 (110 Stat. 1936) (104th United States Congress August 21, 1996).

Hoog, A. (2011). *Forensic Security Analysis of Google Wallet.* San Francisco: viaForensics.

Hughes, S. J. (10 July 2012). *Statement to the Senate Hearing on Mobile Payments.* Committee on Baking, Housing, and Urban Affairs. Washington, DC: U.S. Senate.

iHub Research; Research Solutions Africa. (2012). *Mobile Phone Usage at the Kenyan Base of the Pyramid.* iHub Research; Research Solutions Africa.

Jack, W., & Suri, T. (2011). *Mobile Money: The Economics of M-PESA.* The National Bureau of Economic Research.

Jones, P. (2009, Spring). Rethinking the European Cards Harmonization Framework. *n-genuity Magazine* .

Juniper Research. (2011). *Whitepaper: Mobile Money Goes Mainstream.* Hampshire, UK: Juniper Research.

Katz, M. L. (2012). *Statement to the Senate, Developing a Framework for Safe and Efficient Mobile Payments (Part 2).* Committee on Banking, Housing, and Urban Affairs. Washington, DC: U.S. Senate.

Kimenyi, M. S., & Ndung'u, N. S. (2009). *Expanding the Financial Services Frontier: Lessons From Mobile Phone Banking in Kenya.* Washington: Brookings.

King, N. J., & Jessen, P. W. (2010). Profiling the mobile customer - Privacy concerns when behavioural marketers target mobile phones - Part I. *Computer Law and Security Review , 26*, 455-478.

King, N. J., & Jessen, P. W. (2010). Profiling the mobile customer - Privacy concerns when behavioural marketers target mobile phones - Part I. *Computer Law and Security Review , 26*, 455-478.

Klein, M., & Mayer, C. (2011). *Mobile Banking and Financial Inclusion: Regulatory Lessons.* Washington: World Bank.

KPMG International. (2007). *Mobile payments in Asia Pacific.* Hong Kong: KPMG .

Lachaal, L., & Zhang, J. (2012). Mobile Money Services, Regulation and Creating an Enabling Environment in Africa. *Africa Capacity Development Brief , 3* (2).

Lauer, K., Dias, D., & Tarazi. (2011). *Bank Agents: Risk Management, Mitigation, and Supervision.* Washington: Consultative Group to Assist the Poor (CGAP).

Martin, A. (2010, January 4). How Visa, Using Card Fees, Dominates the Market. *The New York Times* .

Miller, C. (2012). *Exporing the NFC ATtack Surface.* Denver: Accuvant Labs.

Mobile Money Tracker. (2013, 03 2). Retrieved from GSM Association: http://www.mobileworldlive.com/mobile-money-tracker

Montgomery, K. C. (2012). *Statement to the Senate Hearing on Mobile Payments.* Committee on Banking, Housing, and Urban Affairs. Washington, DC: U.S. Senate.

Ndiwalana, A., & Popov, O. (2008). Mobile Payments: A Comparison between Philippine and Ugandan Contexts. *IST-Africa 2008 Conference Proceedings* (p. 10). Windhoek: IST-Africa.

NTT Docomo. (2010). *Press Release: Subscriptions to iD Mobile Credit Payment Services Top 15 Million.* Tokyo: NTT Docomo.

OECD. (2012). *Report on Consumer Protection in Online and Mobile Payments.* Directorate for Science, Technology, and Industry. Paris: Committee on Consumer Policy.

Olivarez-Giles, N. (2012, October 17). Isis Mobile Payments Set for Oct. 22 Launch in Salt Lake City, Austin. *Wired* , p. 1.

Ondrus, J., Lyytinen, K., & Pigneur, Y. (2009). Why Mobile Payments Fail? Towards a Dynamic and Multi-perspective Explanation. *System Sciences HCISS 42nd International Conference on Computing and Processing.* Hawaii: IEEE .

Oosting, I. (2012, September 7). How mobile POS and payment systems prevent fraud. *Mobile Payments Today* , p. 1.

Payment Services Directive, 2007/64/EC (European Commission December 5, 2007).

PricewaterhouseCoopers. (2013). *Mobile payments: Is trust the key to consumer uptake?* Banking and Capital Markets. Toronto: PwC Canada Foundation.

Quorus Consulting Group. (2012). *2012 Cell Phone Consumer Attitudes.* Ottawa: Quorus.

Reserve Bank of India. (2009). *Mobile Payment in India: Operative Guidelines for Banks.* Retrieved from Reserve Bank of India: http://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=1365

Richard, C. C. (2012). Mobile Remittances and Dodd-Frank: Reviewing the Effects of the CFPB Regulations. *Pittsburgh Journal of Technology Law & Policy , 12* (6), 1-24.

Robinson, N., Graux, H., Botterman, M., & Valeri, L. (2009). *Review of the European Data Protection Directive.* Cambridge, UK: RAND Europe.

Rockefeller IV, J. D. (19 May 2011). *Statement to the Senate, Consumer Protection in the Mobile Marketplace.* Committee on Commerce, Science, and Transportation, Subcommittee on Consumer Protection, Product Safety, and Insurance. Washington, DC: U.S. Senate.

Safaricom. (2011, May 6). *M-PESA Customer Agent Numbers.* Retrieved March 18, 2013, from Safaricom: www.safaricom.co.ke

Sang-Hun, C. (2009, May 24). In South Korea, All Life is Mobile. *The New York Times* .

Sotomayor, N. L. (2012, September). Guideline for Consumer Protection in Mobile Financial Services. *Guideline for Consumer Protection in Mobile Financial Services* . Bangkok, Thailand: Alliance for Financial Inclusion.

Sultana, R. (2009). *Mobile banking: Overview of Regulatory framework in emerging markets.* Bangladesh: Grameenphone Ltd.

Surowieki, J. (2008, April 28). Parsing Paulson. *The New Yorker* .

Susswein, R. (2012). *Petition to CFPB Re: Reloadable Prepaid Cards (Docket No. CFPB-20120019, RIN 3170-AA22).* Washington: Consumer Action.

Swedish International Development Cooperation Agency. (2010). *The Innovative Use of Mobile Applications in East Africa.* Helsinki: Edita Publishing.

Telecommunications Act, Pub.L. 104-104 (110 Stat. 56) (104th United States Congress January 3, 1996).

Trichur, R. (2013, march 20). Rogers boosts smartphone offerings in mobile-payment push. *The Globe and Mail* .

Turing, D. (2011). *Payment Services Directive Delayed Onset: Getting Ready for 'D+1'.* Brussels: European Payments Council.

Veniard, C., & Goss, S. (2012). Mobile Payments in the Philippines: Future Opportunities for Growth. *Lydian Journal* (8).

Wack, K. (2012a, March 23). Lawmakers Being to Explore Mobile-Payments Security. *Payments Source* , p. 1.

Wack, K. (2012, March 30). Senate Takes Up Mobile Payments Consumer Protections. *Payments Source* , p. 1.

Weiner, S. E., Bardford, T., Hayashi, F., Sullivan, R. J., Wang, Z., & Rosati, S. (2007). Nonbanks and Risk in Retail Payments. *Join ECB-Bank of England Conference on Payment Systems and Financial Stability.* Frankfurt.

World Bank. (2012). *Information and Communications for Development: Maximizing Mobile.* Washington: World Bank.

World Bank. (2012). *The Little Data Book on Financial Inclusion.* Washington: World Bank.

Zhou, Y., & Jiang, X. (2012). Dissecting Android Malware: Characterization and Evolution. *2012 IEEE Symposium on Security and Privacy* (pp. 95-109). San Francisco: IEEE Computer Society.