12-2018

Privacy Regulations in the Context of Finance: Comparison Between Developing and Developed Countries

Dimuthu Candauda Arachchige Sarathchandra
st cloud state university, dimuthu.sarathchandra@gmail.com

Privacy Regulations in the Context of Finance: Comparison Between Developing and Developed Countries

by

Dimuthu Candauda Arachchige Sarathchandra

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree

Master of Science

in Information Assurance

December, 2018

Starred Paper Committee:
Susantha Herath, Chairperson
Lynn Collen
Nimantha Manamperi

Abstract

Information security and privacy regulation are significant areas of legislation in the financial and micro-finance sectors in the world. There are significant disparities between the developed and developing countries concerning adoption and application of the data protection laws. The developed world has exemplified its laws in the General Data Protection Regulation (GDPR) clause of the European Union that comes into effect on May 18, 2018. In the US, the main law has been the Gramm-Leach-Bliley Act (GLBA) of the late 1990s. The developing countries, on the other hand, exhibit slow drafting of new finance and micro-finance privacy laws and still use policies of the 1990s. The purpose of the study is, therefore, to examine the effectiveness of privacy and data protection laws in finance and micro-finance sectors in the developed and developing parts of the world in the current technological era. The method of the study is a mixed qualitative and quantitative assessment of case studies of recent literature on the subject. Each case study will feature the variables of the presence of privacy laws and information security regulations, and the level of enforcement of those regulations that inform the statistics. The other variable will be the level of effectiveness of the application of privacy and information security laws in developed and developing nations based on case study outcomes. The results indicate that out of 10 examined cases, six show failures of the laws in developing nations while 1 shows failure in a developed nation (South Korea) and 1, in the US, presents mixed results. The recommendations include the adoption of international laws that govern data security in the financial sector, such as the current GDPR of the European of Union.

Table of Contents

Chapter Page

Chapter Page

Appendices

List of Tables

List of Figures

Figure Page

Chapter 1: Introduction

Introduction

The rise in data breaches all over the world makes the prioritization of privacy and information security key amongst various successful enterprises. The interconnected global economy has made it possible to share data across different jurisdictions and create new digital identities (Blum, 2017). For this reason, there is a need for data security laws to fill the vulnerabilities that this interconnected system presents. One of these is the need to propagate new access restriction systems that can reduce breaches of identity theft (Blum, 2017). However, with the stipulated technological flow of information and data, various other aspects of information security and privacy are under crossfire. For instance, the development of consumer relationship technology, intense competition and the need for personalized products has made banking institutions to tap into consumer data (Omarini, 2011). With various developed economies, the above issue will often be considered as a violation of the consumer privacy rights, while in developing countries, the limited regulatory framework does not consider such issues to be impacting or else, critical when facilitating the protection of their citizens. Making a comparison between the data and privacy regulations implemented by most developed states like EU and U.S, Cano (2014) insists that developing countries can limit the occurrence of fraudulent activities in their economies by adopting some of the security measures implemented by regulators like SEC. Laying implicit emphasis on the various supervision and regulatory policies integrated by Microfinance Institutions (MFIs), the research critiques the expected outcomes that the various privacy and data protection policies would have upon developing nations/economies.

The policies used by developed nations, in essence, bring about the improvement of quality services in the financial sector. This is because information security regulation at the private level has involved over 30 years of continuous research in many sectors, including finance, to assess software weaknesses against threats (Schmidt & White, 2017). This has made data protection strong in the United States. However, Schmidt and White (2017), note that despite this proactive approach, major cyber incidents still occur, with a case in point being the Equifax breach of 2017. Analysts touted that the compromise occurred from the use of security programs that were not up-to-date unlike those of the hackers (Schmidt & White, 2017). The outcome brings into question the ability of enterprises to maintain in-house technological maintenance (Schmidt & White, 2017). Data security as such deals with the existing enterprise's ability to determine the manner in which data in a computer system could be subject to sharing with other third parties.

According to Agelidis (2016), under the GLBA law of 1999, information security for financial companies entails the practices that entities enforce to safeguard personal data against external access. It is also an expectation for the companies to offer written evidence to their clients on how they intend to ensure the latter's privacy (Agelidis, 2016). The loss of information and data often occur as a result of unauthorized access, examination, use, modification, disclosure, copying, or moving data/information without customer consent. For instance, the digital disclosure of hacked information publicly has become common due to the mass access to the Internet as a platform for corporate information (Agelidis, 2016).

To enable effective protection levels, the U.S Securities and other industrial policing facilitate the realization of proper regulatory standards, which will essentially mandate the

creation of information security practices at an organizational or national level. The SEC, for example, provides a risk assessment document each year that companies fill to review the threat background in the context of financial losses and customer data breaches (Khan, 2016). Drawing from the above issue, one might conclusively concur that realizing the protection of consumer details, information, and data (mainly, concerning financial statements) requires nations, enterprises, and global corporations (such as WTO, World Bank) to develop security or privacy networks/technologies.

Technology in developing countries, on the other hand, has attracted many small organizations in finance and micro-finance, among other industries (Dahiru & Allison, 2014). Evidence shows that most of the African small-scale enterprises and micro-finance are not as adept as their Western counterparts in the countering of information security and privacy challenges (Dahiru & Allison, 2014). Many first-time ventures into the digital environment often incur cybercrime-related losses (Dahiru & Allison, 2014).

The United Nations Conference on Trade and Development (2016), argues that although African states have evolved regional data protection mechanisms, these are still enshrined in trading pacts. As a result, the eventual outcome of such regional models is uncertain in the current epoch where many countries lack technological resources to keep up with advanced cybercrime (United Nations Conference on Trade and Development, 2016). In Asian countries, there is a growing need to adopt data protection frameworks that go beyond the 1990s, when most of these countries promulgated most of their privacy laws (Yu, 2017). Indeed, most of the implemented regulations have to integrate protections that align with technology and innovative paradigms.

The various industries in developing countries often experience the emerging or else, impacting aspects that correlate to data security and regulations. In this sense, most of the developing world's industries could be said to be inconsiderate of the fact that some industries and business' operational efficiency, essentially calls for significant transformations in sectors such as banking tech. Additionally, the use of Information Technology in various sectors including telecommunication has fawned certain requirement for data protection in banks and other industries (Singh, Picot, Kranz, Gupta, & Ojha, 2013). In such an occurrence or shifts in regulations to compel improvement of operational, enterprise, banking and micro-finance' regulatory standards, as well as, the mitigation of data breaches that are quite prevalent under most financial foundations in developing nations, company or governmental agencies, and other interested lobby groups such as WTO (*world trade organization*) should always involve usage of policing framework and data protection strategies.

Corporate information security interventions and the reporting of data breaches are some of the recommended ways to reduce financial losses and privacy compromises (Laube & Bohme, 2016). Various nations require that companies regularly report all ensuing cyber-attacks (Laube & Bohme, 2016). One corporate intervention is the use of trained employees to run the information security department of a company or to outsource it (Patel, 2008). Either way, studies from outsourcing in India have revealed that both internal and external data protection rules are difficult to follow as they are continually changing (Patel, 2008). One report indicates that one in every five Western companies with either the internal or external data protection model does not comply with data breach reporting requirements due to the ever-changing statuses of the laws (Patel, 2008). A company's regulations, in essence, can facilitate the

increment in efficiency specifically during the identification of unauthorized and external file access. However, unlike most companies operating in developed nations, the possibility of data breaches as well as privacy violations in various developing or further, undeveloped states will always be high corresponding to the challenging conditions experienced at the economic markets/levels.

There is also a low commitment to keep up with new technology in developing countries especially in micro-finance, such as in Asia (Yu, 2017). Despite having a growth rate of ten times in Internet access since the early 2000s, China and other countries of Asia are now coping with outdated laws of previous decades (Broadhurst & Chang, 2013; Yu, 2017). The inability by microfinance institutions to implement usage of better protection mechanisms especially at financial and organizational levels will inevitably bring about the increase in vulnerability to data breaches as well as loss of revenue.

With the rise of mobile and Information and Communications Technology (ICT) framework in developing nations, businesses are not just exposed to traditional market competition but electronic data security (Klimburg & Zylberberg, 2015). This security necessity sometimes comes with a price tag in that it costs banking institutions vital customer data (Klimburg & Zylberberg, 2015). For instance, cyber-attacks, generally at the financial level, have fleeced South Africa five hundred and seventy-three million dollars (Klimburg & Zylberberg, 2015). This is mostly due to lack of a proper data regulatory law. As such, enterprises will only assure data and privacy regulations, if the protection mechanisms used on employees' records, loyalty schemes, customer details/preferences, and finally, data transactions are characteristic of the effective regulatory framework.

Various developing countries like India and South Africa have undertaken policy measures to regulate breaches on financial data against such acts as identity theft and phishing (Cassim, 2015). This is due to the realization that financial companies in both Western and developing nations cannot do without technology which they use to store sensitive data on computer systems (Klimberg & Zilberberg, 2015). In the United Kingdom and the United States, there has been a drive to limit the susceptibility of firms to hacking acts through strong regulation (Cassim, 2015). In the US, the first major such act was the 1978 'Right to Financial Privacy Act' (Cassim, 2015). In the UK, the 'Fraud Prevention Service' (Cassim, 2015) is the law that covers online and financial crimes. In developing nations, like South Africa, there have been few anti-identity theft laws which have led to the mushrooming misuse of credit card data (Cassim, 2015).

The occurrence of phishing, hacking, and therefore, the loss of company, database, and institutional private data could at times be attributable to elements regarding the professionalism of the ‘information security manager.' In developing nations such as South Africa, black hat theft and the resultant financial fleecing of the victims has led to the ranking of the country as the seventh of the fifty most affected nations by the Federal Bureau of Investigation (Brodie, 2014). The vulnerability exists due to the recent accessibility of the web via mobile devices by most South Africans, and for companies using personal computers, the lack of proper security installations gives easy entry to the hackers (Brodie, 2014). For this reason, countries in need of superior economic progress need to install information security systems that match the changing face of technology that hackers easily command (Dlamini, Eloff, & Eloff, 2009). It is clear that

information protection is no longer a vestige for ICT but the entire economic performance of a corporate institution, especially in finance (Dlamini et al., 2009).

Problem Statement

The lack of regulations to safeguard data privacy in developing countries is a serious issue compared to developed countries. These concerns further intensify when considering Microfinance as a sector which is most popular in developing countries where privacy regulations are at a minimum. Therefore, there is a higher possibility of privacy violations in these communities with the increasing involvement of new technologies where large amounts of consumer data are being used. Making an articulation to the privacy concerns that have been rising in the global stage, it will be necessary for companies' especially international corporations such as Apple, to guarantee privacy and confidentiality of customer/consumer data/information. As such, with this research study, the researcher will facilitate the identification of critical privacy regulations in many developing nations as well as some developed countries that ought to be subject to address these issues to ensure the limited loss of data/information.

Research Objectives

1. This research project seeks to highlight through case studies the level of enforcement of information security and privacy laws in both developed and developing countries. The main focus in the developed world will be the implementation of GLBA law of 1999 in the US as well as the impact of the General Data Protection Regulation in the European Union. At least 6 case studies from Africa and Asia will provide details of the level of effective use of the draft data protection laws for the regions' micro-finance and finance institutions.

2. The study will also quantify the level of awareness of privacy and data protection laws in developing countries. Details from such countries as Nigeria, Uganda, and Ghana will provide data on how the customers of micro-finance institutions of the respective nations approach inputting data online.
3. With outdated technology being the major bottleneck of implementation of data protection and privacy laws, it is also the objective of the research to review how financial institutions have kept up with technological changes. Critical areas of examination will be the adoption of a new set of regulations to reflect the switch from privacy laws that were written before the Internet age. The regions under review include Africa and South-east Asia.
4. While comparing the data protection and security policies across developed and developing countries, the study will also examine significant data breaches of recent times. Some of these will include the Morgan Stanley customer data compromise of 2012 to 2014, the South Korea telecommunication hacking, and breaches in Africa.

Purpose of the Study

Advocating for improvement in data security, confidentiality, and privacy is a necessity for any company and governments around the globe. Most data losses in various developing nations usually result in enormous financial losses that in essence impact the economy. With this research study, the comparison between the security and data regulations implemented by developed and developing nations generates the required and significant issues that ought to be addressed to enable the eventual attainment of better global consumer/customer protection mechanisms.

The purpose of the study is to compare data protection and privacy regulation laws of developed countries with those of other countries. The study will examine the European Union's GDPR and the US GLBA, as some of the two key legislation for data regulation, globally. Three foci of the study will be (1) To review the privacy and data protection measures that finance and micro-finance institutions have put up to adhere to privacy regulations of their respective countries or regions. (2) Based on the financial loss magnitude per country's financial sector, it is the purpose of this study to illustrate that most of the losses that occur in such areas as micro-finance or mobile banking take place through lax implementation, misuse or non-existence of such laws (Abdulrauf, 2016). For instance, the study will touch upon Nigeria's $550 million losses as a result of lax enforcement of data protection laws in its mobile banking sector (Baur-Yazbck et al., 2017). (3) The study also seeks to reveal that keeping up with technological changes in the banking sector in developing countries such as Malaysia is a salvaging point for the better protection of privacy in the digital age. It is apparent that many of the developing nations still use their 1990s laws (Shuhidan, Hamidi, & Saleh, 2017).

Finally, it is the purpose of the study, through sample comparisons between developed and developing nations, to reveal that data breaches can still happen internally when an insider leads to the exposure of corporate data to potential hackers (Security Exchange Commission, 2016). Case studies of such breaches will serve as an illustration of the need to come up with new policies in both developed and developing countries to handle information security.

Research Questions

The study will have three research questions, namely:

1. How effective are the information security measures and privacy regulations of developed versus developing countries in the financial sector?
2. As evidenced by the case study results, how effectively have finance institutions enforced the privacy and data protection laws in their jurisdictions?
3. Since part of the reasons financial institutions adopt privacy and data regulation policies is to reduce financial losses, how effective are these based on case study results of financial breaches?

Chapter 2: Literature Review

Introduction

Information security laws differ in diverse demographic and economic regions of the globe. For instance, in much of the developed world, data security laws are an integral mandate for all firms while other nations enforce them for only as much as they shield financial institutions from the legal outcomes of compromises (Miskam & Shahwahid, 2014). Irrespective of the jurisdiction, electronic transfer of banking data and holding the same on servers has become a necessity (Hamidovic, 2014). For the above reasons, it follows that many countries have fawned laws that categorize the identity of such information and the consequences of sensitive data transfer (Hamidovic, 2014). This is out of the belief that information is liable to lose much of its privacy and be prone to diverse kinds of breaching when it assumes an electronic format (Sarabi, Naghizadeh, Liu, & Liu, 2016).

Around 18 individuals suffer from a cyber-spying incident every second, which adds up to the one and a half million worldwide incidents per day (Cohen, 2014). The developing countries suffer most of the brunt because of the lapse of time before the setup of information system laws. For instance, rising economies like China, the Indian subcontinent and some parts of south-east Asia ratified their information security laws as late as early this decade (Cohen, 2014). In the financial sector, the developing world is also the most affected because of bewilderment on which areas to regulate. A case in point is the slow formulation of data laws in certain countries on electronic pay cards (Johnson, Lincke, Imhof, & Lim, 2014). Still, nations like Brazil were as late as 2014 deliberating on regulating cyber laws around these payment systems (Johnson et al., 2014). Another South American nation, Argentina, by 2013 still had not

put in place particular clauses to govern Internet privacy through ensuring protection on cookie information and sensitive consumer data (Craig et al., 2013).

Even in the first world nations, there are still high likelihoods of data manipulation, especially during the introduction of new networks. For instance, Australia has a privacy law, but it is not as strict as the EU counterpart in that a financial institution does not have to inform the authorities of every act of mining consumer data as long as the latter is notified (Craig et al., 2013). The proposal to offer uncharged public scale Internet also poses a threat to information security, despite the existing strong laws, due to multi-network routing (European Union Agency for Network and Information Security, 2014). One such system that is set to roll out in Europe in the mid-2020s sets out to offer zero-charged Internet to the public of the member states (Pham, Galic, & Taylor, 2017). The inherent threat is that public cyberspace is easier to breach when it is free for everyone to access than one secured intranet (Pham et al., 2017). In light of the above details, this literature review will focus on holistic international privacy laws and how they apply to two key related sectors. These include financial institutions and micro-financial institutions. The scope will be the developed and developing world. Each section will offer the latest literary input on the subject.

Financial Industry and Micro-finance

The first area in which to explore the financial industry as it is cognizant of privacy laws in the United States. The financial sector is a key driver of the country's economy (Mohammed, 2015). This is the reason the GLB Act of 1999 specifies that US banks ought to notify customers on how they intend to handle their private data (Walrath, 2017). The Act governs how banks disseminate private data to external agents that the customer does not directly relate to,

especially about security cards and account details (Mohammed, 2015). Its strengths include full disclosure by banks to clients (Walrath, 2017). Despite being more advanced than similar acts in developing nations, there are limitations of this law's applicability in a changing financial context (Walrath, 2017).

In Europe's financial sector, some of the strictest rules on information security are already in force (Baker, 2016). Not only do banking institutions get into the spotlight in their own countries but in the European Union economic bloc (Baker, 2016). For instance, the very core of their businesses, namely the acquisition of customers is under scrutiny from the various angles of privacy, fraud, and ethics (Baker, 2016). Even when customers are likely to be the perpetrators of the crimes, some laws, like the United Kingdom's PRA, delve into the accountability of a bank in its behavior to its clientele. This is in recognition of the opinion that a profit-making entity may manipulate consumer data unscrupulously for gain (Baker, 2016).

The financial industry in developing nations faces serious information breaches due to still immature policies. In South Africa, for instance, data compromises are inside jobs that involve banks' Information Technology staff (Ngcamu, 2016). A case study by Ngcamu (2016), highlighted that the dearth of non-disclosure contracts led to staff misuse of information outside the company. The financial institution in question also was a pacesetter in not apportioning information risk as a part of its risk management mandate (Ngcamu, 2016).

Another developing world context is that of Indonesia. The financial institutions of the south-east Asian nation still concentrate on the past laws that govern cyber data and privacy (Palupy, 2011). Most companies still utilize the outdated clauses despite the quick disruptions in software that have visited upon the banking sector in recent years (Palupy, 2011). Across the

borders, Singaporean and Indonesian banking sectors are having to bow to governmental pressure to sufficiently protect their consumers. In Singapore, the laws are evolving from mainly governmental controls to flexible regulations that allow private financial institutions to join the latest protection initiatives (Palupy, 2011).

About the micro-finance sector, developing nations' micro institutions struggle to survive due to both financial and poor regulatory matters (Fotabong, 2012). For instance in Cameroon, since early this decade the failure rate of major companies in 2010 not necessarily affiliated to data breaching has led to increased government involvement to avert future closures (Fotabong, 2012). A primary method of affordable technology that micro-financial institutions in Cameroon use are mobile, which due to its widespread use generates a high level of data vulnerability (Mwafise & Stapleton, 2012). One of the major reasons for the adoption is the development of a telecom-based money remittance system (Mwafise & Stapleton, 2012). The same study found that of all the factors that led to the widespread utility of the service, privacy (at 96.8%) and restrictions to user data (92.5%) came at numbers four and five after such factors as simplicity (100%), confidentiality (100%) and trust (Mwafise & Stapleton, 2012). This highlighted that privacy is still in the developing stage even in the users' contexts in the country.

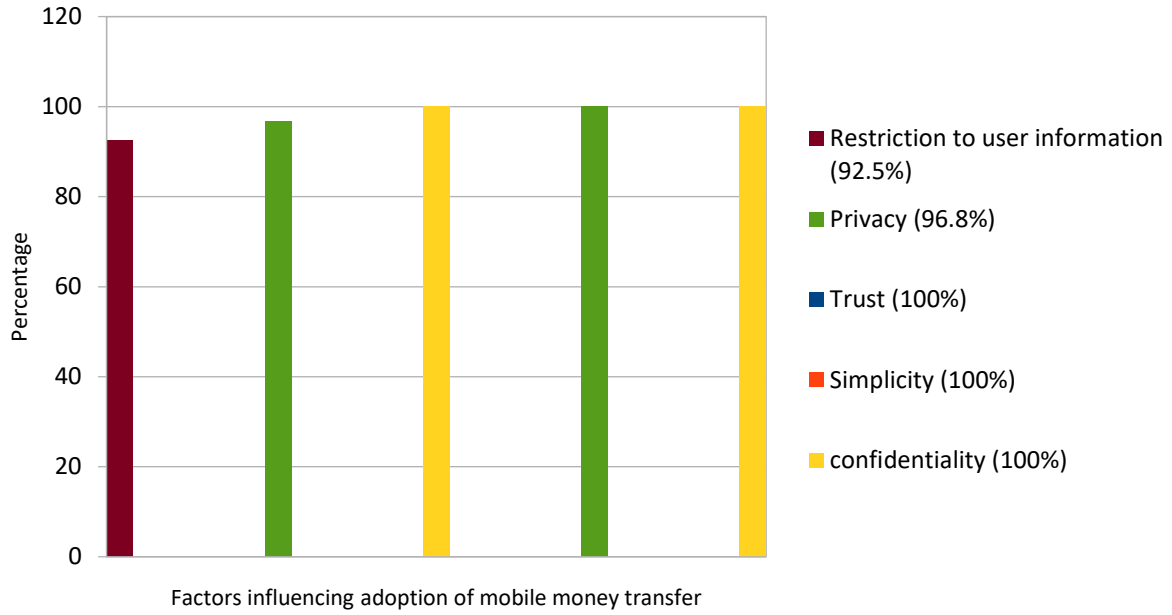


Figure 1: Factors influencing the adoption of mobile money transfer in Cameroon.

In developed societies, such as Europe, the major information security factor that governs the few operating micro-institutions' data security is a WiFi network (European Union Agency for Network and Information Security, 2014). The networks that most banks use includes WiFi which if unsecured with passwords poses privacy risks for the users. The fact that many financial bodies have operations across country boundaries means multi-jurisdictional access to customer data and hence multiplied vulnerability. To overcome these variances, the European jurisdictions have sought to unify the information security bills to overcome conflict of interest, across borders (European Union Agency for Network and Information Security, 2014). Due to the advancement of cyber laws in the EU setting, what remains is to secure the loopholes in the networks, which means the routing paths that information flows from small institutes to large banks after customers send in their requests (European Union Agency for Network and Information Security, 2014). The figure below illustrates the exposed network paths.

Therefore, even as financial and micro-finance institutions execute various measures to ensure data privacy, there are still missing gaps in both developed and developing nations.

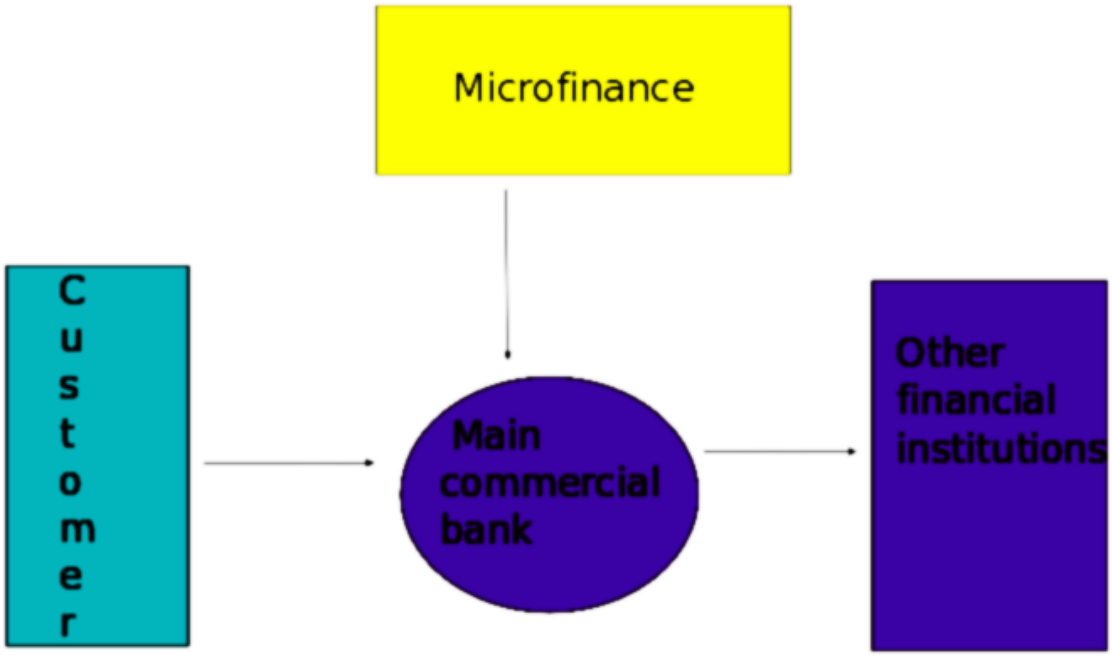


Figure 2: Sample financial institutions network path.

The world, for instance, the connectivity of data along multiple bank communication paths increases the manifold severity of a breach should it happen (Camillo, 2016; European Union Agency for Network and Information Security, 2014). Studies in recent times reveal that banks that take a trio of steps, inclusive of in-house, external and network harmonization can stem the tide of network breaches (Camillo, 2016). This is especially true of companies that operate in a highly interconnected system that demands different legal implementation of conflicting information security protocols.

International Privacy Regulations

The modern privacy laws have a foundation in Scandinavia. In 1973, Sweden published its initial privacy clause, which set the way for other countries to prepare similar all-encompassing laws (Booysen & Neo, 2017). By the first quarter of 2016, a hundred and ten similar bills had become institutionalized in as many nations. This was more than two additional nations per year that ratified their laws similarly (Booysen & Neo, 2017). Banking institutions were the first to embrace this form of information security through their in-house tax and cash revenue matters (Mello, 2012). They would soon find complications when they crossed borders as each sovereign state had a law a little different from the home country, ideally meaning that unscrupulous secrecy would not work (Mello, 2012). This is despite the fact that privacy laws serve the same objective (Booysen & Neo, 2017).

Privacy laws in all sectors began in earnest in the 1800s when governments would use records to surveil over their citizens (Solove, 2006). The request for privacy details during each population count led to grumbling about privacy. The institutionalization of law in the second half of the 1800s to cease invasion of public data in the United States' census was one outcome of this trend (Solove, 2006).

The first evidence of laws governing technological breach of privacy was in the liberal age of the 1960s (Kenyon, 2016). One such act was the use of extensions to record another party's telephone messages, which led to privacy clauses against telephonic tapping (Solove, 2006). The 1990s saw the rise of the Internet with equal fear of financial breaches during the dot.com era, and the US GLB Act was a culmination of decade-long online confidentiality acts

(Walrath, 2017). The primary law of the current century is the EU privacy or GDPR which will apply fully in 2018 among European member states (Allen & Overy LLP, 2017).

Table 1

Comparative Timelines of the Medium and Use of General Privacy Laws from the 1800s to 2010s

Timeline of Privacy laws	**Medium**	**Use**
1800-1899	Paper records, post & telegraph.	State surveillance (Solove, 2006).
1900-1960	Public systems, telephone, state records.	To prevent legal privacy torts and to enhance federal espionage (Solove, 2006).
1960-1990	The constitution, information acts of the 1960s, espionage privacy laws of the 1970s, computer laws of the late 1980s and audio-visual privacy laws of the late 1980s (Solove, 2006)	The rise of the '60s technological liberalism led to numerous constitutional acts while the coming of the computer led to the ratification of new laws (Kenyon, 2016; Solove, 2006).
The 90s	The Internet	GLB Act (1999) in the US and numerous web-based privacy bills (Walrath, 2017).
2000-2018	Internet, cloud	Numerous privacy acts on security after 9/11 (Lane, 2014). The EU's new Internet privacy laws are coming into effect mid-May 2018 (Allen & Overy LLP, 2017).

One of the remarkable problems of the current international privacy regulations is the lack of harmonization across countries (Allen & Overy LLP, 2017; Bu-Pasha, 2017). This is important especially in the background of the fact that much data is seamless and universal to apply due to the development of a similar Internet worldwide (Bu-Pasha, 2017). The latest offering to bridge this gap is the harmonized EU law that takes effect in mid-May, 2018 (Allen & Overy LLP, 2017). From that date, all continental privacy framework will supersede the select country equivalents (Allen & Overy LLP, 2017).

Despite emanating from the biggest financial and trading duo in the world, US privacy legacy is markedly disparate from its European counterpart (Movius & Krup, 2009). The US emphasizes local financial institutions, but it does not have as stringent regulation as the EU (Movius & Krup, 2009). Therefore, whenever there are tradeoffs of information during a cross-Atlantic deal, any consequences of privacy become challenging to resolve unless there is court intervention (VanWasshnova, 2008). For instance, the discovery of the 2006 clandestine passenger espionage program by the US in Europe led to the condemnation of privacy data breaching by the court (VanWasshnova, 2008). This is despite the two continents putting enough protection measures against financial breaches in their respective institutions (Movius & Krup, 2009).

Just like the rest of the world has different information security and privacy bills, so are developing countries. In Africa, principally Lesotho, the laws are still in the development stage despite being encompassed in a regional bloc (Makulilo & Mophethe, 2016). The country passed its latest act in 2011, but this would likely undergo revisiting after regional bodies like the

trading community of South African states evolved policies and required member countries to update theirs (Makulilo & Mophethe, 2016).

Naude (2014), states that South Africa has had a poor record in the enactment of privacy clauses to keep its digital citizenry safe. However, a 2013 bill sought to transform the country's track record with the entrenchment of international elements (Naude, 2014). These included the perpetual updating of the laws to stay up-to-date with the ever-upgrading technology that leaves behind old laws (Naude, 2014). A case study in 2008 of the biggest users of computers, comprising of corporate leaders, technology personnel and other employees in South Africa found that restriction to computer access by outsiders was only enforced at 57% levels (Stander, Dunnet, & Rizzo, 2008). However, the biggest means of protection were Internet security programs at a level of 98% (Stander et al., 2008). Fifty-three percent of participants also indicated that their security personnel enforced data protection checks (Stander et al., 2008). Despite this outcome, the study concluded that the legal protection mechanisms do not read the same page with the technological changes responsible for the breaches (Stander et al., 2008).

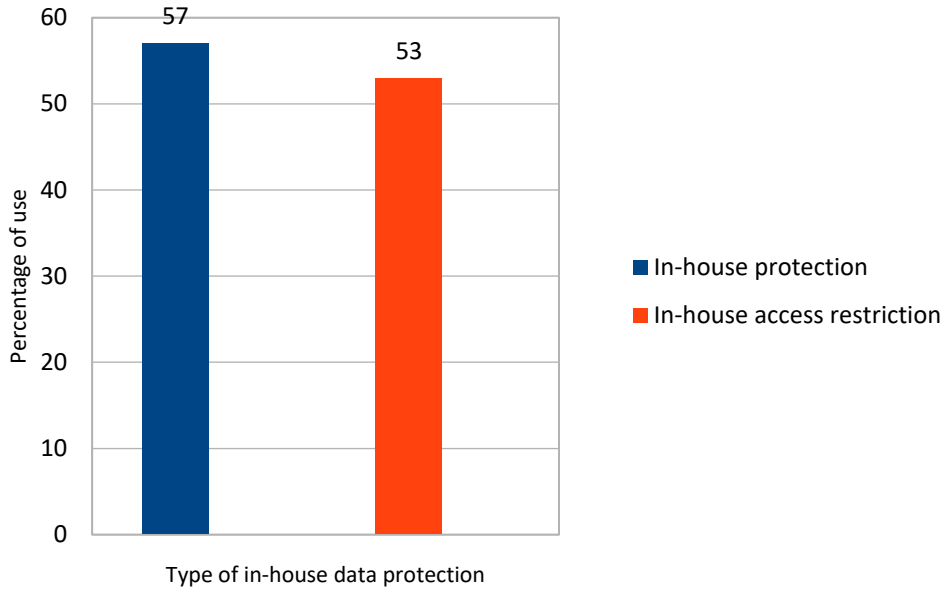


Figure 3: Type of in-house data protection in South Africa in 2008.

In short, though there is a rising global need to shield the privacy of users in, especially sensitive fields like finance, the international regulations have been pragmatic (Sorensen, 2017). Each state except for regional bodies, like the EU, have fawned different jurisdictional frameworks (Bu-Pasha, 2017). Harmonization will be the one recommendation for filling the gap of these different laws that regulate similar devices, software and data breaches worldwide (Bu-Pasha, 2017; Sorensen, 2017).

Privacy Regulations and Policies in the Finance Sector

The rise of soft money remittances is one of the major factors for privacy regulations in the finance sector. For instance, in 2016, five hundred billion soft cash exchanges took place around the world, which acted as a catalyst to the need to safeguard the senders' and recipients' data (Carbo-Valverde, 2016).

For the above reason, a country-by-country review on privacy rules on banking can provide new insights into the importance governments have placed on online banking. For instance, Singapore's 2014 promulgation on the individual's right to information security provided that a business that spammed a client with unwanted e-commerce missives would elicit a monetary fine (Raul, 2014). In the same year, Russia imposed mandatory upkeep of all data, financial or otherwise, within the country's servers (Raul, 2014). China would follow suit with a cybersecurity law that came up in 2017 that stipulates the localization of secret information (Brink, Wang, Veldhoen, & Arnbak, 2017). The epitome of all privacy laws remains that of Europe's 'Data Protection Regulation' (Raul, 2014), which many other nations have either tried to imitate or shunned, altogether.

The major privacy regulation law in the US is GLBA. It regulates the disbursement or storage of consumer data by banks (Sheng & Cranor, 2012). It also governs the use of factual data, puts a limit on workers' information access by outsiders and expects banks to install information security processes to keep data safe (Sheng & Cranor, 2012).

A 1999 to 2005 longitudinal survey on the pressure finance sector players in the United States face from the enactment of GLBA law revealed mixed outcomes (Sheng & Cranor, 2012). Though many banks were of the view that information regulation was paramount to safeguard consumer information, there was counter-argument for the need to relax the rules (Sheng & Cranor, 2012). The study concluded that even in the US the regulations did not have much effect as small finance entities still shared customers' data with affiliated companies (Sheng & Cranor, 2012). On average, the largest ten finance institutions and retail outlets in the survey shared

consumer data one hundred percent with affiliates, 40 to 80% with non-affiliates and gave consumers opting-out options of between 40 and 100% magnitudes.

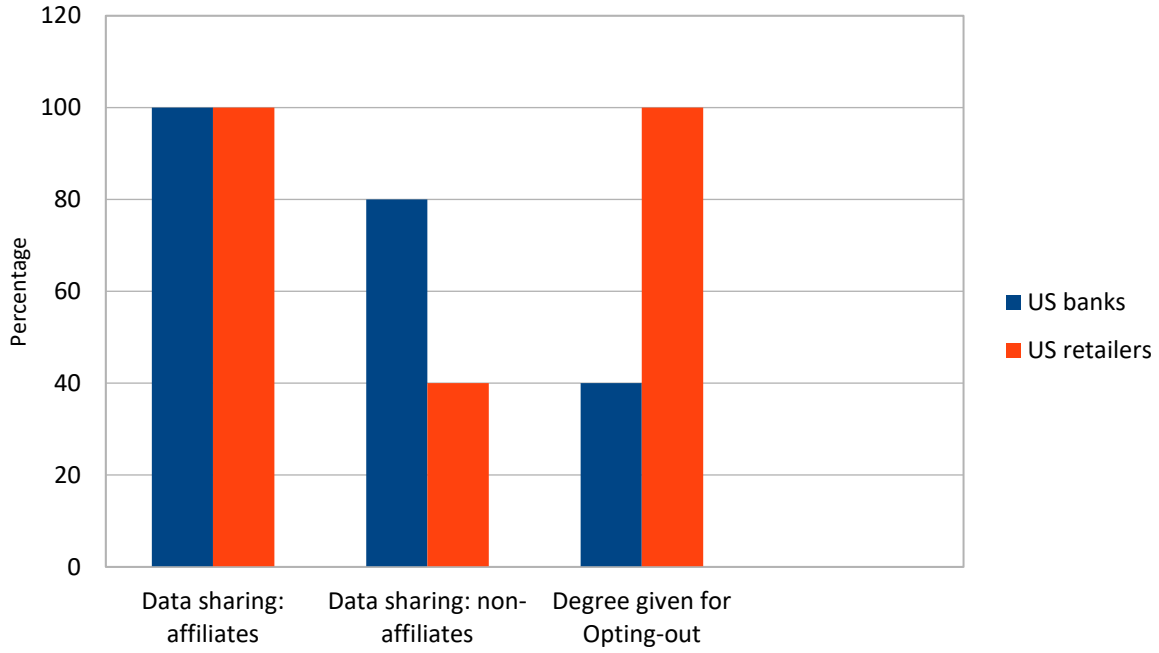


Figure 4: How banks and retailers transfer data with affiliates and non-affiliates in the US.

Another important legal recourse for consumers about travesties on their privacy by outsiders or banks is the 'Electronic Fund Transfer Act' (Mohammed, 2015). It came about as a result of the increase in non-cash remittances (Carbo-Verde, 2016). The law is under implementation in diverse states in different forms including in governing mobile and electronic card transactions (Budnitz, 2016; Mohammed, 2015). It covers all kinds of gadgets, some of which are hinted upon such as smartphones when they feature in financial issues involving user information (Budnitz, 2016). The privacy policy of EFTA is to the effect that the custodians of the points of sale and automated teller machines notify the authorities in situations where consumer data undergoes unscrupulous access (Mohammed, 2015). This is important because

automated payment devices are not manned and thus may not have a person directly responsible for stolen information (Mohammed, 2015).

Privacy policy and regulations in developing countries are significantly behind those of the developed ones. For instance, South Africa has the ECT Act of the early 2000s that still governs how e-banking takes care of web consumers (Kabanda, 2010; Mtuze, 2015). It is interesting that before 2002 when the law came up, the country's e-bankers had no clear guidelines on how financial communique online held the sender legally liable to the message (Kabanda, 2010). The gist of this new clause is that Internet portals of institutions engaged in e-commerce ought to have overt and covert manifestations on how they maintain the confidentiality of their clients' information (Mtuze, 2015). The overt part is the presence of privacy policy widgets at the nether part of banks' online databases to reveal their exact stand on client data protection (Kabanda, 2010). A survey by Kabanda (2010), in the late 2000s, found that South Africans had very low trust in their banking data repositories as they felt that the institutions only enforced select ECT stipulations.

In Nigeria, the privacy laws exist, but they are blunt to the essence that institutions only enforce them by having a privacy officer in place (Patricia & Izuchukwu, 2014). The first fully-fledged legal recourse that captured the modern rise of technology in finance was 2006's e-banking rules or 'E-Electronic Banking' (Ezeoha, 2006). They laid out grounds for broad areas of Internet-based breaches of information security not covered before (Ezeoha, 2006). Despite the law, the country's banking institutions still carry out the 'know your clients' (Abdulrauf, 2016) policy as a formality, sometimes without regard to the regulations. This is a precondition that for the banks to provide optimal services, they ought to mine some necessary data of their customer

base without breaching their privacy. Often, they take extra information which amounts to a contravention of the stipulations on client protection (Abdulrauf, 2016).

Asia's developing economies such as that of India are also behind their Western peers, mainly European, on privacy policies around finance (Jamil & Khan, 2011). India ranks as one of the biggest outsourcing nations globally and hence the high need for banking institutions to safeguard users who transact trade online (Directo, 2014). The existing act is 'IT Act 2000' (Jamil & Khan, 2011). It underwent new amendments in recent years following the promulgation of PDPB, a bill that came up to the national assembly in 2006 to offer EU-like privacy on all aspects of online life, not just banking (Jamil & Khan, 2011). In a 2011 survey, 26% of CFOs in corporations around the world specified India as the best country for offshore task delivery (Directo, 2014). The same survey also unveiled that Western entities could easily alter this preference and seek outsourcing elsewhere were India's privacy laws not to change from their developing phase (Directo, 2014).

Some of the very different recent privacy laws are from emerging economies, principally China. The country in 2017 promulgated its collective set of regulations on 'cybersecurity' (Brink et al., 2017). What is disparate from its Western counterparts is that the regulation is highly information security-oriented in that it targets data compromises that come from outside its national borders (Brink et al., 2017). For this reason, the law stipulates that individuals and banks keep their sensitive data in country-based servers rather than abroad (KPMG, 2017). Another stipulation is that although financial institutions and individuals may have the right to keep their information confidential, the state has the power to request for data that it deems sensitive (Brik

et al., 2017). Table 2 summarizes the new stipulations for financial and other entities operating within China in 2018.

Table 2

China's New Cybersecurity Law of 2017 Summary

Regulation	**Effect**
Internal data protection	Use of better data protection methods through the installation of information security systems for China-based companies. (Brink et al., 2017).
Personnel	Recruitment of information security personnel or network operators, per business, to enforce network protection (Brink et al., 2017; KPMG, 2017).
Privacy	Storage, transmission and consensual use of customer data per the new law (Brink et al., 2017)
Privacy across borders	Institutions to keep in mind the probability of information being leaked, lost or spied upon by foreigners and thus the need for in-country storage (Brink et al., 2017; KPMG, 2017)

The above section has highlighted that the sector still needs to promulgate more laws to keep up with the changing face of online banking, especially in upcoming markets in Africa and Asia. Zahoor, Ud-din, and Sunami (2016), reiterate this point in their report that the finance sector attracts more hackers than all other industries. The latest minefields of consumer data that criminals go on to use; include electronic payment devices, automated teller machines, and even direct leakage of a customer's banking identity (Zahoor et al., 2016).

As the case of China's new privacy regulations show, it is a legal expectation to maintain consumer data internally through the employment of data security officers (Brink et al., 2017). For this to happen in developing nations, which are currently ill-equipped to meet the challenge, there needs a training program by the banks on data protection (Tse et al., 2013). Through their survey on global banking institutions that implemented such education, Tse et al. (2013) found that in 2012, no more than 47% of the participants had put in place training initiatives to handle data enlightenment for their staff members. Of these, 37% set their information security and privacy policies to guide their third-party relations on data protection (Tse et al., 2013). Therefore, it is apparent that global financial institutions need vibrant training of their staff as a starting point to realize their privacy aims.

Privacy in the Micro-finance Sector

The regulation of micro-finance institutions takes many forms and mostly affects the developing regions of the world. Despite this essence, data privacy is still informal in many countries (Egboro, 2015). In Nigeria, for instance, while there are ethical approaches by major banks to client data, these rules do not apply to micro-finance (Egboro, 2015). Indeed, these institutions discuss consumer data in boardrooms, which puts the data at risk of leakage (Egboro, 2015).

The nearest equivalent in the EU is e-banking and mobile transactions, which the E-money ordinance already covers (Pouchous, 2012). The law guides for a limited period of the retention of customer details after which it undergoes annihilation (Lumsden, 2013; Pouchous, 2012). In the United States, the closest form of micro-finance is also mobile finance. It is essential in privacy regulations emanated from the fact that by 2013, cellular gadgets had

replaced existing telephones per home by a margin of 31.6% (Lumsden, 2013). Whereas in the EU companies have a finite time of keeping consumer data after which it is deleted, in the US firms can hold confidential details of cellular subscribers indefinitely (Lumsden, 2013). For this reason, legal agitators in the country have been calling for a stricter law than the current one about the exact period to keep such sensitive data until it is destroyed (Lumsden, 2013).

To govern information security in e-banking, the US currently enforces the 'Cyberspace Policy' (Lumsden, 2013). In privacy and mobile telemarketing, the US Federal Communications Commission (FCC) rule provides many stipulations on the use of limits to consumer data. For instance, marketing directly ought to have an opt-in or out option imposed on network companies, but this does not apply to non-affiliates (King, 2008). Though, it is criminal for the latter to use the data to pretext consumers (King, 2008). The use of consumer information is an on 'as is' basis, which implies that the mobile banker can store and transfer the customer's details but only up to the limit where there is personal consent (King, 2008). There is no regulation for non-affiliates and manufacturers of gadgets though it is criminal to pretext (King, 2008). The chart below outlines the above stipulations.

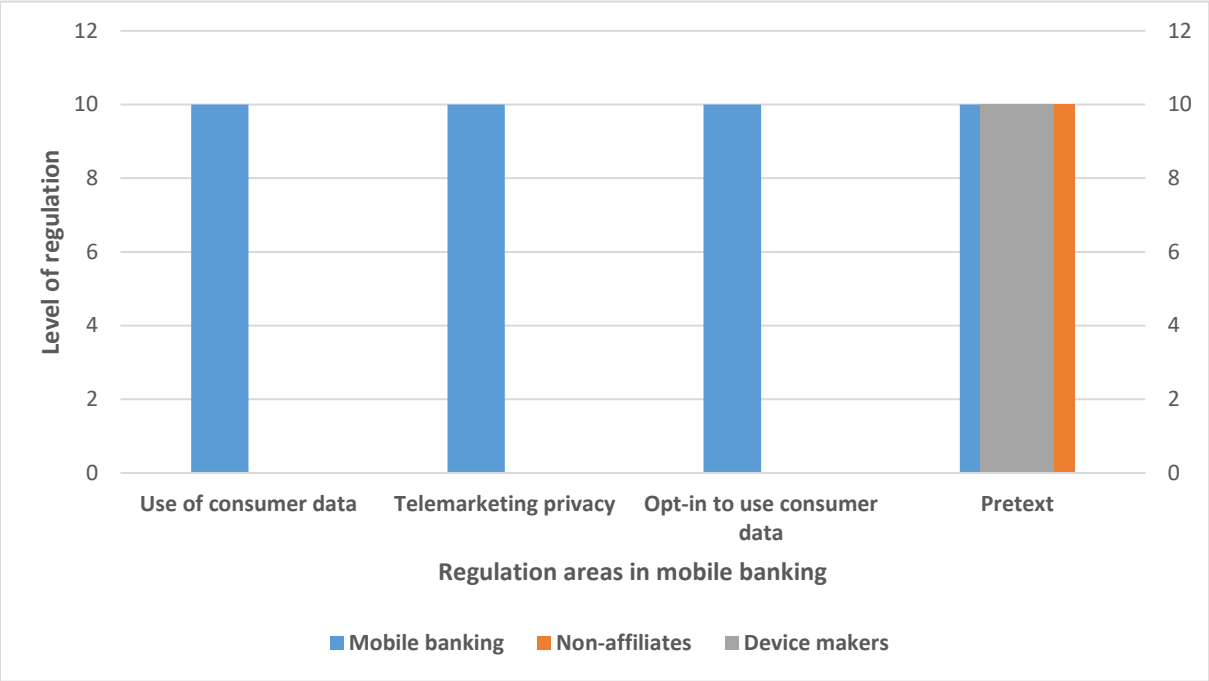


Figure 5: Regulatory areas in mobile banking in the US.

In most parts of the developing world, bills to protect clients' information privacy have been snail-paced in comparison to their European e-banking counterparts (Pouchous, 2012). Only states in south-east Asia such as Indonesia have been on the forefront in recent years to promote privacy and other protection policies due to the rapid digitization of the micro-finance niche (Pouchous, 2012). In Kenya, the development of mobile payments has also colluded with over-dependence on the mobile device as a banking tool (Pouchous, 2012). However, the very simplicity of mobile utility puts the often technologically uninformed Kenyan customer at risk (Pouchous, 2012).

Sub-saharan Africa is one of the critical regions as far as micro banking is concerned to cater for the low earnings bracket in need of banking (Arun & Murinde, 2010). The introduction of privacy regulation has been embraced since the late 2000s due to the emergence of electronic

and phone-based transactions that may undermine data confidentiality (Arun & Murinde, 2010). One of the factors that are under regulation is the social capital of the client. For instance, in Mauritius, there is a clause that gives microfinance institutions the ability to process the user's data to find the latter's eligibility to access the banking service. The clause also guides on the limits of such an investigation (Arun & Murinde 2010). Most other nations in the continent apart from South Africa had no such law in 2010 (Arun & Murinde, 2010). Nigeria, on the other hand, lacks laws to specifically regulate the microfinance outlets despite their being present in many cities (Oluyombo, 2007). The country's 1952 law on banking bypassed mention of the term 'microfinance' and so do latter-day clauses in the late 2000s (Oluyombo, 2007).

Uganda, on its part, despite the proliferation of new forms of micro banking has been a slow implementer of privacy laws. By 2016, there was still a lack of an information security clause to govern privacy (Privacy International, 2016). The country's information docket proposed such a bill in 2014, but to date, the passage of a drafted copy is yet to come to light (Privacy International, 2016). The country's governing privacy laws are mostly international in nature and surround issues on human rights rather than data (Privacy International, 2016). Ugandans are most likely to disclose their private details to banking sites only when there are over details that enhance trust, including the presence of a privacy statement on the website's page (Mwesigwa, 2010). There has been low progress in embracing e-banking because of doubts about privacy regulations and the perceptions of low information security online by the majority of the unbanked customers (Mwesigwa, 2010). Due to the lack of such laws, the reliance on perceptions on risks has become the main indicator of whether to use an online banking service or not in Uganda (Mwesigwa, 2010). The diagram below illustrates such perceptions.

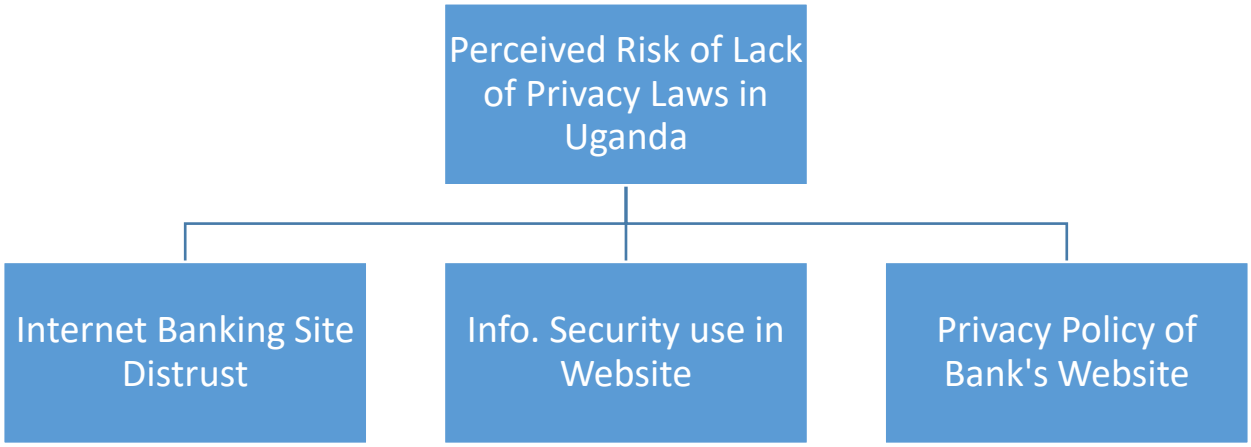


Figure 6: Risks due to lack of privacy laws in micro-finance in Uganda.

In South American nations, micro-finance is under regulation albeit in mainly financial points of view such as deposit disclosure information (Ardic, Ibrahim, & Mylenko, 2011). Chile, however, passed the 1999 law known as 'Protection of Privacy' (Ardic et al., 2011). A recent proposed update to the bill was to the effect that banks, micro or large, still using outdated laws and needed to translate them to the technological age (Carey & Silva, 2016). Table 3 comparatively summarizes the latest points that the new law stipulates.

Table 3

Privacy Data Laws on Micro and Mainstream Banking in Chile

1999 Privacy Law	**2016-17 proposed update bill**
The law specified written acceptance to banks' use of consumer data.	This may change from 'written' to technological transmission of data in the digital banking age (Carey & Silva, 2016).
The current privacy regulation has no clear definitions of what is exempted from client consent to give details to banks.	The new law may configure if consent exempts such currently undefined purposes as the in-house use of customer data, among others (Carey & Silva, 2016).
Unconditional consenting exists in the current law.	Unconditional consenting will receive an update to include client acceptance of the use of their data by institutions, via diverse mediums like the internet (Carey & Silva, 2016).

In Asia, privacy laws have been around since the 1990s, but they are still developing in many countries (Greenleaf, 2014). In Taiwan, there have been many instances of fines imposed on small and large banking venues for breaching consumers' sensitive data (Greenleaf, 2014). A case in point was when two banks faced fines that amounted to a hundred and thirty thousand dollars separately. Their reason was for the exposure of their clients' banking details to criminals who hacked into their systems (Greenleaf, 2014). Thus, there are ties between information security and privacy in Taiwanese laws. Around Asia, the term privacy has multiple meanings, but each country interprets it through its court system, which determines what constitutes data compromises, especially when there are doubts (Greenleaf, 2014; Kershaw, 2014). This is because there are usually few precedents to use due to the rapid progress of technology that requires regular updates of privacy rules (Kershaw, 2014).

In the Philippines, all rules are governed by the 'Data Privacy Act 2011' (Government of Philippines, 2014). The adoption of the law was the first of its kind as it embraced the many

entities with online databases including state and private (Government of Philippines, 2014). The clause concerns universal information confidentiality, but it applies to the microfinance sector in the way the institutions mine and disburse clients' data (Sahu, 2018). The clause stipulates that the micro-banking institution can only gather and transfer personal details under the authorization of the customer who is the official custodian of such information (Sahu, 2018). The law defines the confidential data as familial, spiritual, ethical or stance-related. It also categorizes personal health status as a part of banking details that can only be transferred through the individual's consent (Sahu, 2018).

Information security and privacy have become inseparable in recent times due to the increment of breaches even in the microfinance setting. Gyabi and Shrivas (2016), presents a case of how community banks in a West African context find ties between privacy and information security. In a Ghanaian rural background, the government enforces information technology policies to streamline confidentiality and to ensure the low vulnerability of microfinance clients' data (Gyabi & Shrivas, 2016). Thus, it is a requirement that community-level small banks to carry out frequent system auditing to assess the likelihood of system attacks.

The above case study assessed that the small financial outlets found system threats insurmountable and even in situations where a hacking act happened, they might not necessarily be well equipped to alert the customer of the outcome (Gyabi & Shrivas, 2016). The survey on a broad number of customers in the above setting returned the results as follows: 37% of the respondents replied that the strongest privacy and data protection policy their small banks enforced was the password. 17% identified the DataPro software as in use by their microfinance institutions to mitigate information leakage. Only 12% replied that there was a strong use of an

access restriction rule, while 9% specified that their small banks had computer usage policies (Gyabi & Srhivas, 2016). The chart below highlights the above results from the survey.

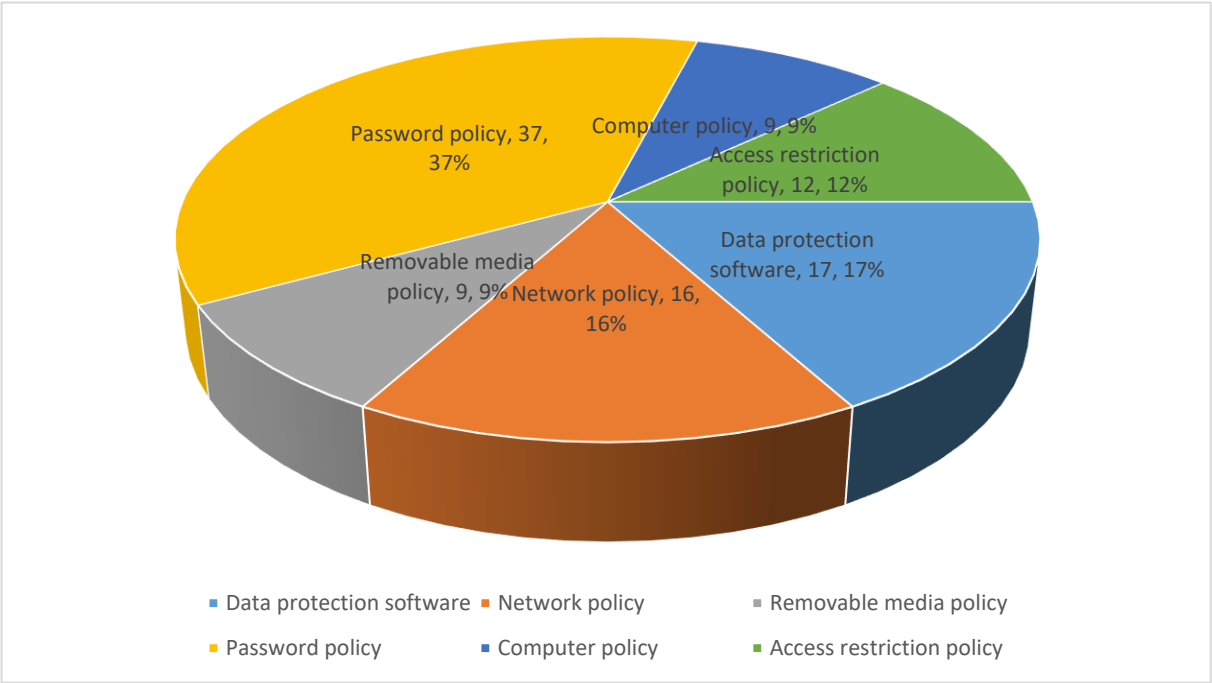


Figure 7: Survey results in Ghana in 2016 on information security and privacy measures in rural microfinance.

Therefore, micro-finance, despite being a catalyst for development in the unbanked communities of the Third World, poses a threat to consumer data due to the slow implementation of data protection regulations. Most rules in South America, apart from Chile, are broad sweeping and do not have reconnaissance on the changing phase of online privacy in microfinance (Ardic et al., 2011). In Asia, despite efforts by some states to implement the laws to keep up with the alterations in cyber technology, some countries still use their 1990s' policies (Greenleaf, 2014). African states are still underdeveloped in microfinance laws, and in certain countries like Uganda, the rules are yet to exist even though the institutions bank the majority of the rural customers (Mwesigwa, 2010).

The Conclusion to Literature Review

From the above sections, it is apparent that information security and privacy is one of the most important measures that banks and microfinance institutions currently implement (Hamidovic, 2014). The study has enunciated the prevalence of strict laws in the European Union that safeguard the keeping, retrieval and the deletion of a customer's sensitive information. The economic bloc also currently has one of the strongest set of privacy rules in the world that member countries will superimpose over their sovereign legislations by mid-May 2018 (Allen & Overy LLP, 2017).

In the United States, data protection is mainly a mandate of the GBL Act of 1999 which came up at the height of the dot.com era (Sheng & Cranor, 2012). The law still applies even today despite lax conformity by some finance outlets due to the rise of new forms of technology (Sheng & Cranor, 2012). One of these is e-banking, which is the closest form to microfinance in the developed world.

The literature has revealed that the bulk of privacy non-implementation is due to either bank laxity or lack of the rules in the developing world. Nigeria's micro-finance establishments, for example, treat consumer details in an open manner not only during transactions but in board discussions (Egboro, 2015). In Uganda, a 2014 proposed privacy bill be yet to come into law two years later (Privacy International, 2016). Though efforts are apparent in south-east Asia, where countries are instituting bills to replace old 1990s' laws in the background of new technology, the sector is yet to unfold in comparison to the West (Greenleaf, 2014).

Chapter 3: Methodology (Mixed Method Approach)

Introduction

The study will entail a mixed methodology with both quantitative and qualitative elements. The research will review case studies from Internet sites, databases, and peer-reviewed journals. Each section will compare the enforcement of information security or privacy laws in sample cases in developed and developing countries. The first variable will be the presence of privacy laws in the country under the case study. The second variable will be the degree of enforcement of information security in the country under the survey. The dependent variable will be the degree of effectiveness of privacy laws according to the adoption by microfinance or finance sectors of the given jurisdiction. The effectiveness measure can include low information security breaches.

Case Studies on Financial Sector Privacy

Case study in a developed country. In the US in 2015, Morgan Stanley faced an allegation for breaching the data of hundreds of thousands of customers through an internal worker (Federal Trade Commission, 2015). The case's complexity emanated from the fact that the banking institution had implemented all privacy rules per the United States GBLA and other FTC guidelines. It was also notable that the access of sensitive data was limited to staff members up to the extent that they needed it for corporate purposes (Federal Trade Commission, 2015). The complication came up because the worker exposed over seven hundred and thirty thousand accounts to professional hackers (U.S. Securities and Exchange Commission, 2016).

A case in point was that the individual was able to access the report repository and transfer the data to an intranet database at a personal residence (Federal Trade Commission,

2015). The data would later find its way into dongles and other individual gadgets, a contravention of the bank's privacy policies (Federal Trade Commission, 2015). From there it dispersed online through a third-party act of hacking where the affected individuals' details were under auction (U.S. Securities and Exchange Commission, 2016). The federal body intervened to rule whether to follow the banker's counterargument of one of its workers inadvertently hacking criminally into its system or whether the banker was responsible for the exposure of a client's privacy through weak data storage.

Tesco bank breach–UK. In November 2016, Tesco Bank was subjected to a hack that saw £2.5 million stolen off from 9,000 of its accounts in what some security experts are describing as the most serious, attack ever to hit the United Kingdom's banking sector. As described by Frost (2017) in her article, the attack is believed to have encountered through its online banking system, affecting 20,000 accounts in total. The attack had targeted a weekend, where banks are generally slow to react to online threats while the stolen money was then used to buy thousands of goods from worldwide retailers using the contactless mobile-phone payment method.

As put forward by Jones (2016) in the article on the guardian website, the author claims that as found by an academic team the criminals have used merchants' payment websites to guess people's card details. More elaboratively the criminals use software that automatically generates different variations of a card's security data–for example, the card number, expiry date and three-digit security code known as the CVV–and fires these off to hundreds or even thousands of websites around the world at the same time. The reply to the transaction would confirm whether or not the guess was right.

The bank had adhered to the Regulation 61 of the Payment Services Regulations 2009 in the UK and paid refunded its affected customers £2.5 million. The regulation above requires a bank to refund the amount of an unauthorized payment transaction to the payer and to restore the debited payment account to the state it would have been in had the unauthorized payment transaction not taken place. Furthermore, UK's Financial Conduct Authority (FCA) could have considered the breach of Principle 3 of its Principles for Businesses. Under this principle, a firm must take reasonable care to organize and control its affairs responsibly and effectively, with adequate risk management systems. This will raise questions as to whether adequate protection against the risk posed by evolving forms of cybercrime was in place at Tesco Bank. If a failure in this area is established there is the possibility that the bank will face a substantial financial penalty, although this has been yet to be decided.

Australia: AAPT hacking case study. In a case study published by Palfrey (2013) discusses the attack, and the implication under previous and new laws, which targeted the Australian Internet Service Provider AAPT resulting in customer data was being hacked and published on the internet.

The data exposed by the anonymous hackers was held on a server managed by WebCentral Pty, Ltd, a web-hosting business unit of Melbourne IT. Under the contract between AAPT and WebCentral, WebCentral was required to adequately manage and maintain the server, except for the custom application content and data, which was the responsibility of AAPT. The hackers accessed the data through this customer application named “Cold Fusion” while AAPT was using an old version of Cold Fusion, which was known to have vulnerabilities. When

Melbourne IT became aware of the attack it notified AAPT, which immediately disconnected from the network and took steps to ensure the data could not be further compromised.

As put forward by Palfrey (2013) Australian Privacy Commissioner, Timothy Pilgrim, found AAPT had breached the Privacy Act in respect of the incident. More elaboratively Under Australian National Privacy Policy (NPP 4.1), an organization is required to take reasonable steps to protect the personal information it held from misuse and loss and unauthorized access or disclosure. The question in this scenario was whether AAPT or WebCentral held the data. The Commissioner took the view that AAPT held the data despite it being stored on WebCentral's server. Accordingly, AAPT had the obligation under NPP4.1. The finding of this case study will be discussed further in Chapter 4.

Case study in a developing country. Adelola, Dawson, and Batmaz (2015), surveyed in Nigeria to discover the locals' views on information security and privacy. The study concentrated on all aspects of privacy, but from the outset, the authors warranted that the majority gave privacy a financial connotation. The dependent variables included the instruments the individuals used that put their data at risk including e-banking, e-commerce and traditional banks' websites (Adelola et al., 2015).

The survey consisted of 51% male and 49% female respondents, a total of 72. They were of banking ages of between 20 and 50 years, with the majority (41%) being 20 to 29 years of age. The highest education qualification of the participants was the Bachelor's level at 42% while the lowest was a certificate, at 1 percent (Adelola et al., 2015).

The main questions of the survey (see Appendix B) included the following abridged ones:

1. Do you ever get concerned about the data you offer online?

2. Have spam messages from non-affiliates to your bank ever keep you on the alert on your data?
3. Are you knowledgeable of identity theft and its consequences?
4. Is the state reliable as a custodian of privacy of individual information?

All the questions concerned mostly financial institutions that most of the surveyed group dealt with online and the authors considered them equally important to the respondents (Adelola et al., 2015). The chart below indicates the main classifications of privacy that the above four questions highlighted:

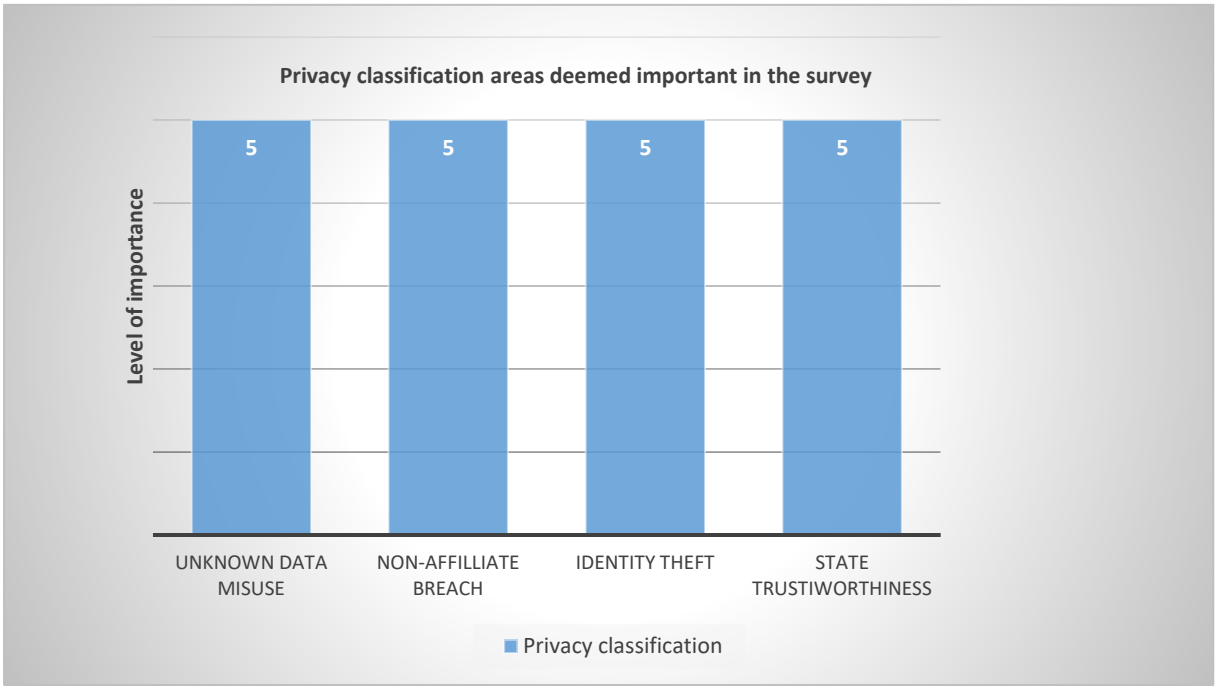


Figure 8: Main areas of privacy concerns among Nigerians, Adeola et al. (2015) survey.

Case Studies on Microfinance

Survey from Asia. Shuhidan et al. (2017) carried out a study in Malaysia on mobile banking security. The sample microfinance customers who used mobile banking received electronic questions on many aspects including privacy. The questions on privacy read, in

abridged form: 1] How do you feel about your private information being used by mobile banks? 2] Are you of the view that your mobile banking data is at risk of hacking?

The study groups consisted of demographically exposed users of micro-finance technology such as m-banking, in the age bracket of 20-39 (Shuhidan et al., 2017). They numbered 384. Two hundred and six of these were male while a 178 were female. Among the dependencies of the survey was the educational attainment of which 72.7% had a degree and 27.3 a postgraduate degree. None had a personal business but the majority, at 82.3%, worked in private capacities. All used smart devices for communication and financial needs (Shuhidan et al. (2017).

Among the preliminary concerns which the study identified that contributed to the main issue of privacy was the fact that they feared the loss of their data via faulty transactions that would hurt their social relations (Shuhidan et al., 2017). It is interesting that the survey also asked the respondents of other factors outside privacy that affected them. The performance was the main question, and it attracted a response rate higher than that of privacy (Shuhidan et al., 2017). (For results see discussion section). Appendix C presents the questions of the survey.

Survey from Africa. To underscore the ease of breach of privacy in microfinance sectors in developing countries, the following details present a survey of the number of microfinance and informal banking customers in several African countries. A study by Maimbo, Faye, and Triki (2011), found that there is no easy categorization of microfinance from informal savings outlets. Thus, there is a high likelihood of some uncategorized institutions to escape privacy laws (Maimbo et al., 2011).

For instance, the survey found that in countries like Kenya, 33% of the respondents did not have any financial affiliation, while 26% were in microfinance (Maimbo et al., 2011). In Malawi, on the other hand, the majority of the surveyed were informal financial institutions, at 55%, while 19% of the participants were in microfinance. In Namibia, 2% were in microfinance while 52% were unbanked. Uganda had 42% of microfinance respondents while 33% had no financial affiliation. The respondents from Zambia were 14% from microfinance while 65% were unbanked (Maimbo et al., 2011).

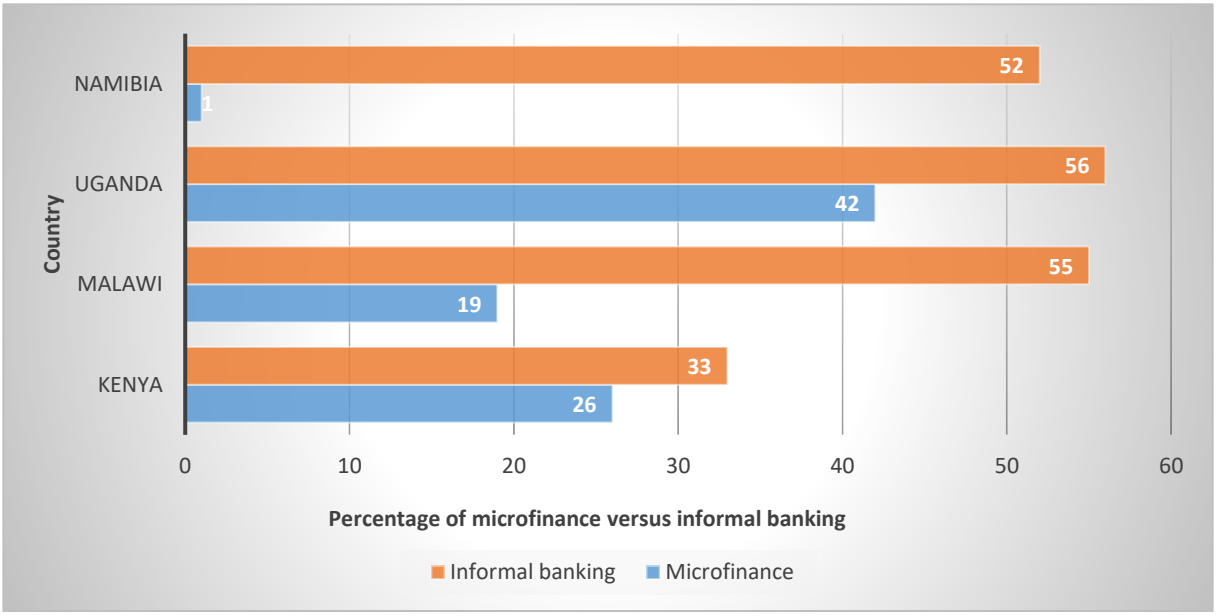


Figure 9: Microfinance vs. informal banking as per survey respondents by Maimbo et al. (2011).

A case study in rural Ghana by Gyabi and Shrivas (2016), sought to partake of rural financial institutions due to their small-scale operations against their information security and privacy measures. A sample area of Ashanti in interior Ghana served as the background for the study. The scope of the research was thirty thousand total customers. However, the research focused on particular service providers and mixed the workers', managers' and customers' input in the questionnaire-based survey (Gyabi & Shrivas, 2016).

The main questions of the survey in abridged format included the following:

1. Which data privacy policy does your company have?
2. Which was the last date when your bank updated the data breach action guideline?
3. Does your financial outlet undertake mock information recovery tests to prepare for breaches? Appendix D has the full questionnaire format, while the findings are in the next section.

Case Study on the Variable of Information Security in Microfinance

According to a report by Baur-Yazbeck, Jenik, and Valenzuela (2017), the lax regulatory framework on micro-finance and particularly mobile banking has affected negatively on East African and West African countries. The study highlighted the effect of the following information security variables: (1) the impact of data identity theft via mobile banking, (2), the level of 'social engineering' (Baur-Yazbeck et al., 2017) during transactions, and (3) virus are planting on clients' mobile devices.

The study then used the data to estimate the total effect, in monetary terms, of the lax information security regulations. The preliminary estimate for the entire of Africa's mobile banking was two billion dollars' worth of lost finance (Baur-Yazbck et al., 2017). That of Ghana was fifty million dollars (Baur-Yazbeck et al., 2017). The full results of the report are in the findings section and Appendices E & F.

Case Study on the Variable of Privacy in Microfinance

Privacy in Myanmar came under the test in 2004 when the state passed a law that required the enforcement of a data protection clause for online certificate revelation to unmask criminals. The open certificate would be inclusive of the user's identity details and secret codes

during an online sign in, under the 'Electronic Transaction Law" (Myanmar Center for Responsible Business, 2015). Before that date, the closest law on privacy was the general mention of the term in the country's constitution (Myanmar Center for Responsible Business, 2015). MCRB surveyed seventy-three corporate sites, most of which were in microfinance. The researcher formulated evaluation criteria that constituted the following set of model questions or their equivalents:

1. Did the companies have in place an explicit privacy statement or data on how they would handle their clients' and stakeholders' information?
2. How many of the 73 entities had their privacy statements embedded as part and parcel of their corporate ethics and mission statements?
3. How many of the 73 companies had put into place sufficient data protection information that a visitor to the website could easily consult?
4. How many entities of the seventy-three had not implemented any privacy regulations on their sites? (Myanmar Center for Responsible Business, 2015).

Appendix G has the above information in the tabled form.

Failed Privacy Laws in Financial and Microfinance Sectors

Failed privacy policy case in a developed country. In developed countries like South Korea, privacy laws have ever failed to protect 85% of all web users in the country that log in daily and input private data (Mendel, Puddephatt, Wagner, Hawtin, & Torres, 2012). In June 2011, around thirty-five million subscribers of a communication company via which they used their financial and other personal data lost their data after a hacking incident (Mendel et al., 2012). The hacking took place in two major customer channels, namely the social media

extension of the company and its search architecture. The reasons for the compromised data might have been the requirement by the state on the use of SSN by customers before they could log in (Mendel et al., 2012). In other words, the breach was occasioned by the very privacy laws that sought to protect the bank and the personal data of consumers. Overall, 70% of native Koreans and 90% of all residents of the country suffered from the hacking breach (Mendel et al., 2012). The chart below presents the salient details.

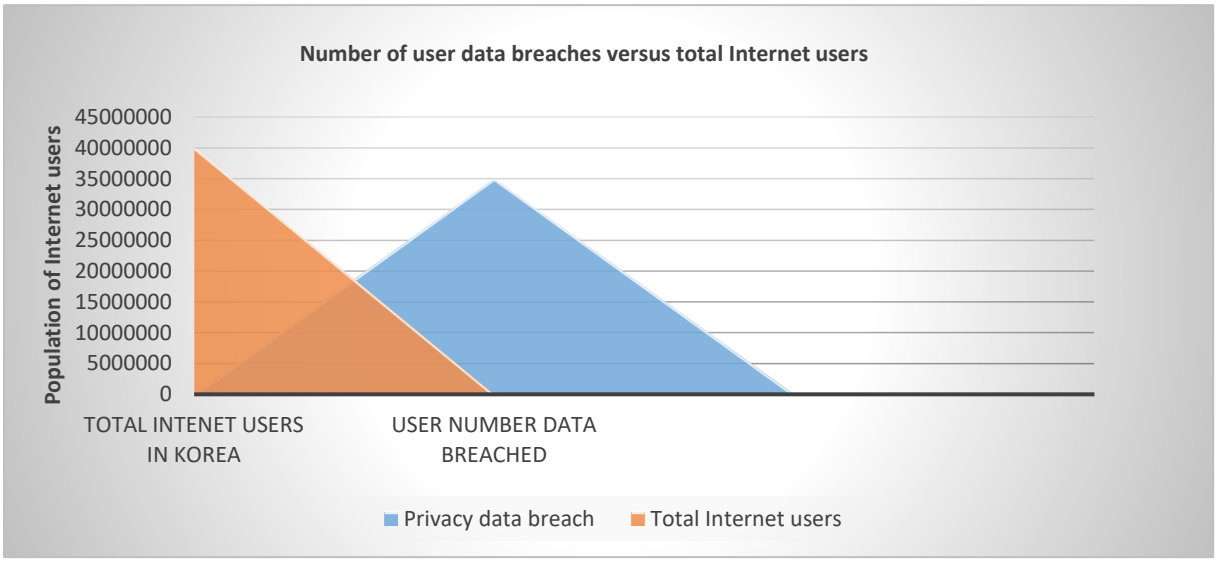


Figure 10: Number of users affected by the breach and total internet users in 2011 in South Korea.

A failed case study in microfinance in developing countries. As a part of a report on global trends on microfinance privacy breaches in the form of cyber-attacks, Mommens (2016), presented the case of Senegal in three years. Between 2014 and 2016, the Sahel nation saw its biggest micro-finance institutions suffer breaches alongside their governmental and bank counterparts. The study presented the effects of the compromises in three contexts that included (1) consumer data vulnerability due to weak regulation and (2) direct loss of money saved in affected accounts. The third one was poor trust as a result of the delayed acquisition by

microfinance institutions of the technology to prepare their customers for breaches. The outcome of the above case study was to the effect that data laws in Senegal, with the latest one being of the year 2008 (Boshe, 2016), have been ineffective as the attacks took place only half a dozen years later. The table below presents the three variables above and their effect on Senegal's 2014 to 2016 micro-finance breaches.

Table 4

Reasons Behind Data Breaches in Senegal

Reason for privacy and data breach in Senegal's microfinance	**Outcome**
Weak regulation of privacy and data protection laws	Loss of sensitive client information (Mommens, 2016).
Direct loss of money in accounts	It accounted for 80 percent of all information security breaches of microfinance in the study period (Mommens, 2016).
Low trust by banks on technology	Due to the heightened rate of cyber-attacks, micro-finance institutions have been left behind from developing in tandem with technology (Mommens, 2016).

From the above sample studies, there is a reflection of accountability despite ongoing data compromises in developed nations. It is apparent that the heart of contention for most developed countries is whether to adopt stronger laws, like the European ones than they currently have or not (Movius & Krup, 2009). For instance, in the Morgan Stanley breach of 2014, the Federal Trade Commission (2015), concluded that the bank had implemented both its rules and GBLA rules of the United States. The Security and Exchange Commission (2016), questioned on the enforcement of written data privacy laws in the bank.

The case study problems in this section have also shown that most developing nations in Africa and Asia still have outdated privacy clauses and are playing catch with cybersecurity. It is apparent that countries like Senegal still have breaches in micro-finance security in the current decade despite passing the 'Data Protection Act' (Boshe, 2016; Mommens, 2016). There is also a widespread lack of concern about the sprouting informal banking institutions such as mobile banking all over Africa. The latter institutions lack privacy laws like those that govern micro-finance (Maimbo et al., 2011). From the evidence of customers' distrust of online banking and the lack of awareness about the undue exposure of their private data, developing countries are still recording poor data regulations (Bauer-Yazbeck et al., 2017). For instance, Nigeria has suffered a massive five hundred and fifty million dollars' worth of losses in micro-finance and micro-banking alone from cyber incidents (Baur-Yazbeck et al., 2017).

In light of the above foreclosing assessment, the following section will present the full results of the above surveys and will offer discussions around the salient points such as privacy laws.

Chapter 4: Findings and Discussion

The following are the findings in consecutive order of the case studies presented in the Methodology section. Each survey follows a discussion about the current privacy and information security laws. The latter clauses will aid to interpret the results.

Findings on FTC (2015) and SEC (2016)

The case in question refers to the breach of consumer data through an internal worker of Morgan Stanley in the United States from 2012 to 2014. The Federal body for privacy and cyber regulations in the United States found that Morgan Stanley had implemented the necessary controls for the preservation of the clients' privacy (Federal Trade Commission, 2015). The other point was that the accessibility of information was only for business reasons, and the use of external dongles by the workers was prohibited. The third point of the findings was that the company had put in place stringent surveillance to assess the rate at which the staff disbursed client information and the volume of such an exchange (Federal Trade Commission, 2015).

The immediate results were to the effect that the bank's worker breached a tiny repository that was the only one that the company had not well maintained (Federal Trade Commission, 2015). This indicated a minor information security breach that FTC found severe but which it allowed passing as the banker immediately overhauled the repository after the breach. It was also notable that the compromised private information was in a system that had not received a security update like the rest and highlighted that privacy and information security is a perpetual process (Federal Trade Commission, 2015). Appendix A has the tabled results of FTC's closure of the case.

A year later, another body in the United States for protecting consumer rights offered a one-million dollar fine on Morgan Stanley (U.S. Securities and Exchange Commission, 2016). The bank would also dismiss the worker responsible for the breach. The findings of the securities body were different from that of FTC in these respects: guilt, documentation, and seriousness of the privacy breach. The table below explores the securities body's latter-day findings:

Table 5

The SEC Findings which Indicated that the US Bank had Inadequate Privacy Policies

Privacy and data breach Count	**SEC Ruling**
No policy in written form.	The company had no written regulations and needed to come up with them (U.S. Securities and Exchange Commission, 2016).
The severity of the breach.	The breach was severe as it took place in a continuous period of three years, ending 2014 and affected nearly three-quarters of a million accounts (U.S. Securities and Exchange Commission, 2016).
The guilt of poor authorization system on data restrictions.	The company had maintained the same authorization programming on its network for a decade, which made it possible for retrieval of data for reasons other than business purposes (U.S. Securities and Exchange Commission, 2016)

Discussion. Two prominent points have come up in the above two findings: (1) what constitutes a severe data breach in a developed country and (2) the internal data protection mechanisms that measure the degree of privacy implementation by a financial institution.

On the first point, the US Act of 2007 on identity theft applies because the large breached accounts could easily pass into the hands of Internet impersonators (Johnson et al., 2014), this affects information security as it applies to a cyber-threat. It also affects privacy in equal measure as it leads to the possible sale of customer data (U.S. Securities and Exchange Commission, 2016). Indeed, the seriousness of the case was that some of the consumer details after the breach were on offer online (U.S. Securities and Exchange Commission, 2016).

On the second point, it is apparent that unlike many similar cases in the developing countries, the US bank had some vibrant internal security mechanisms according to the earlier ruling by the Federal Trade Commission (2015). However, as the securities body argued, the bank may not have put enough internal control to restrict access to sensitive data (Securities Exchange Commission, 2016). Therefore, there was what one may call an effort on the part of the US bank but which did not fully satisfy the privacy law.

Findings on Tesco Bank Breach–UK

In 2016 United Kingdom saw 20,000 of Tesco Bank's customers have their money stolen during a sophisticated cyber-attack which was probably the most significant data breach that the UK's banking sector has faced at that time.

As Vovk (2016) points out that despite some links to fraudsters abroad, there is a possibility that there was probably a mole inside Tesco Bank helping the thieves. The exercise conducted on the bank's system shows that it is tough to penetrate and remotely access a bank's network without assistance from inside, whether it was done deliberately or happened by mistake.

UK's Finance, insurance, and credit institutions were regulated by the Financial Conduct Authority (FCA) in terms of data protection guided by the Data Protection Act 1998, however with the introduction of The EU General Data Protection Regulation (GDPR), those institutions have to comply with rules and regulations by both FCA and GDPR.

As Davis (2018) states, fundamentally the GDPR requires that an organization must now directly inform individuals of what it does with their data–where and how it collects the data, how it is processed, and to whom it is given. The organization has duties to make this communication when it first collects data about individuals and when it changes how it will use that data in the future.

The GDPR, as with the earlier data protection legislation, deals only with data about living individuals, not business data. Data from which individuals cannot be identified, for example, anonymized data, is not subject to the restrictions of the legislation. The legislation primarily applies to a data controller–the organization that "determines the purposes and means of processing personal data." Some obligations are also placed on a data processor–an organization that "processes personal data on behalf of the controller" (Davis, 2018).

Discussion. Showing the active nature of UK's privacy regulations on financial institutions the case of Tesco Breach is considered by the Financial Conduct Authority (FCA) as a possible breach of Principle 3 of its Principles for Businesses. As Charlesworth and Stanton (2016) point out under this principle, an organization must take reasonable care to organize and control its affairs responsibly and effectively, with adequate risk management systems. This raised questions as to whether adequate protection against the risk posed by evolving forms of cybercrime was in place at Tesco Bank. Although the wording is not yet finalized on this case if

a failure in this area is established there is the possibility that the bank will face a substantial financial penalty.

Furthermore, Tesco Bank's regulatory problems may not be limited to compliance with FCA, as the Information Commissioner (ICO) in the UK is also taking an interest. While the ICO currently only has the power to issue monetary penalties of up to £500,000,

> When the General Data Protection Regulation (GDPR) comes into force in 2018, banks will have more reason to worry about the ICO. Penalties for serious data breaches under that legislation could be up to 20,000,000 EUR or for an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. (Charlesworth & Stanton, 2016)

Apart from the aforementioned facts which gives evidence that UK has quite strong data protection regulations in place which only got stronger with the implementation of GDPR in May 2018, the law on unauthorized payments, Regulation 61 of the Payment Services Regulations 2009, requires a bank to refund the amount of an unauthorized payment transaction to the payer and to restore the debited payment account to the state it would have been in had the unauthorized payment transaction not taken place. Hence it is safe to say the UK is largely on top of things regarding having regulations in place and implementation in case of an incident like the Tesco Bank breach.

Findings Australia: AAPT Hacking Case Study

As Srinivas (2015) described in his article, in Australia there are few cybersecurity-related legal, legislative and regulatory obligations applicable for all industry sectors including government agencies. Table 6 below lists those laws.

Table 6

Australian Privacy-related Laws

Australian Privacy Principles (APP)	The APPs are intended to regulate the collection, holding, use and disclosure of personal information. The APP applies to government and private institutions with more than AUD 3 million annual revenue.
Cybercrime Act	Offers comprehensive regulation of computer and Internet-related offenses such as unlawful access and computer trespass, damaging data and impeding access to a computer, theft of data, computer fraud, cyber-stalking, etc. Enhanced the applicability of search and Seizure provisions relating to electronic data.
Spam Act	Established a scheme for the regulation of commercial email and other electronic messages.
Telecommunications Act	Enacted with the objective of protecting the privacy of individuals who use the Australian telecommunication system.

Although Australia lacks industry-specific data protection laws recently, they have brought forward the below regulation which took effect on January 1st, 2017.

> APRA Prudential Standards–CPS 220 (Risk Management) and CPS 231 (Outsourcing). These require APRA regulated entities to have proper risk management strategies, including IT systems, and to ensure that they properly manage outsourcing risk about material business activities, respectively. (Clarke, 2016)

In this case of AAPT breach, the Australian Privacy Commissioner has given the verdict that AAPT had breached the privacy act as they held the data despite it being stored on a third party, WebCentral's, server. Mainly, AAPT had the obligation under Australian Privacy Policy 11.1 which states in circumstances where an agency outsources the data storage; it will still be

likely to be regarded as holding the information under the new provisions and have obligations to protect the information.

Discussion. As evident from the AAPT case study, Australia has quite strong privacy policies although they lack industry-specific privacy laws. Australian Privacy Policies (APP) cover a wide range of privacy concerns and the authority figure of a Privacy Commissioner also gives more weight on privacy protection.

In this particular case study, the Australian Privacy Commissioner took the view that the Primary company AAPT is responsible for the breach even though a third-party company named WebCentral held the data breached. As discussed by Palfrey (2013) the Commissioner found AAPT failed to take reasonable steps to secure the personal information as required by the National Privacy Policies. Specifically, The Commissioner identified several deficiencies in the security of data provisions in the contract between AAPT and WebCentral including:

- Data was not assessed to determine whether it included personal information and its sensitivity
- Existing or emerging security risks were not required to be identified and addressed,
- Vulnerability scanning and the effectiveness of the Cold Fusion application was not required to be undertaken (Palfrey, 2013).

Moreover, in this occasion, the Privacy Commissioner had conducted an own motion investigation as a response to the media reports of this incident, which means that in Australia agencies are not relying on the fact that they have not received a complaint as an indication that any privacy breaches will not be pursued.

Findings on Adelola et al. (2015)

The results of the survey by Adelola et al. (2015), concerning the views of Nigerians on data privacy online highlighted a typical scenario of developing countries, namely unconcern for the governmental laws and minimal awareness.

The responses by the 72 participants on the question, “do you ever get concerned on the information you offer online?” were as follows: 20% said they did all the time, while the majority, at 44%, confirmed that they did so occasionally. Another 24% reported that they speculated about their information quite often (Adelola et al., 2015). The chart below highlights the full results.

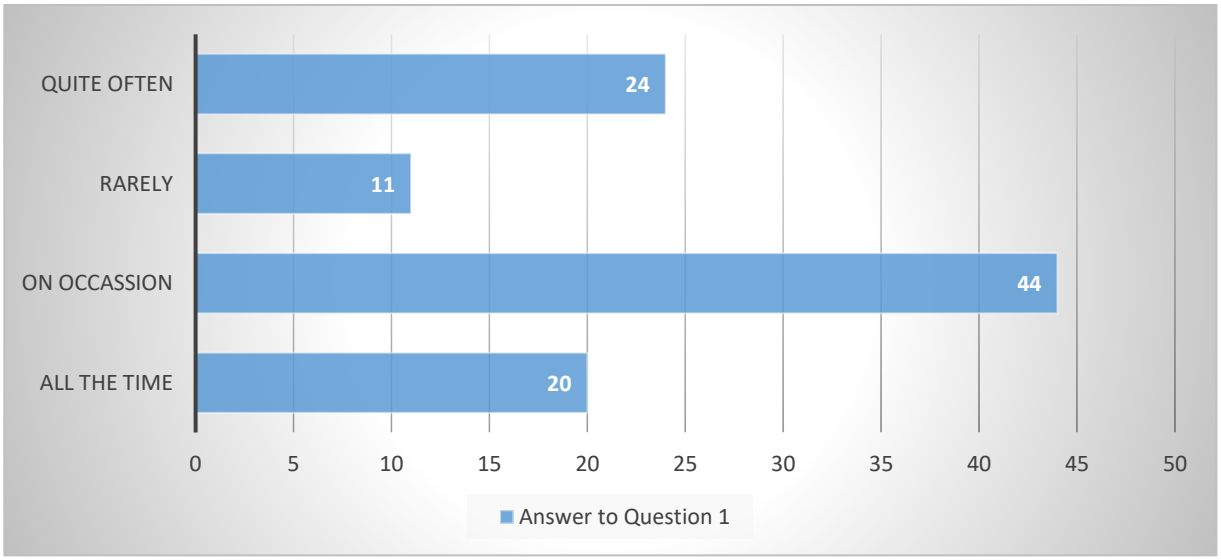


Figure 11: Nigerians on data privacy online, Adelola et al. (2015) survey results.

On question 2, "have spam messages from non-affiliates to your bank ever keep you on the alert on your data?" the answers were as follows: 38% were concerned all the time, while 37% were bothered on occasion, 20% feared quite often, and 6% not at all as the chart below illustrates:

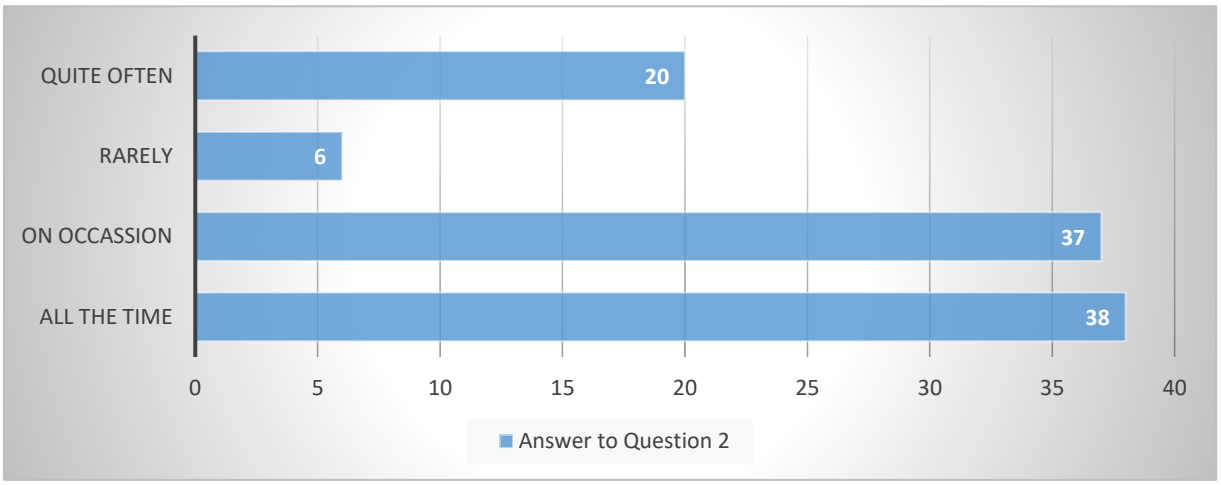


Figure 12: Nigerians survey results about unsolicited non-affiliate spam messages, in Adelola et al. (2015) survey.

About the third question on "are you knowledgeable of identity theft and its consequences?", The results were as follows: 75% said they were aware while 21% were unsure and 4 percent knew nothing. The chart below depicts the data:

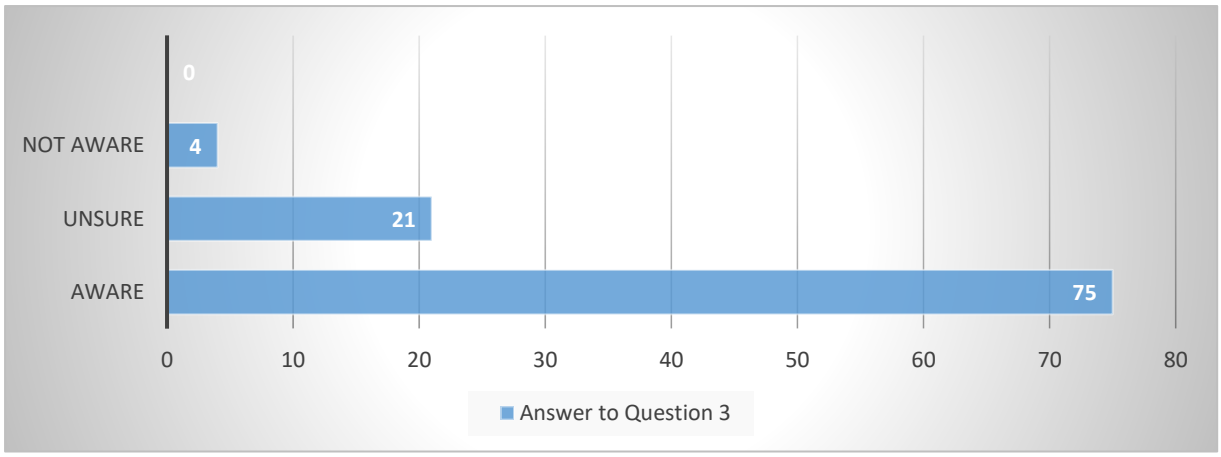


Figure 13: Nigerians awareness of identity theft according to Adelola et al. (2015) survey.

Regarding the final question to the effect, "is the state reliable as a custodian of privacy of individual information?", the results were as follows: 17% had a strong 'no,' 36% were unsure, 16% said 'yes,' while 31% simply said 'no.' The chart below has the details:

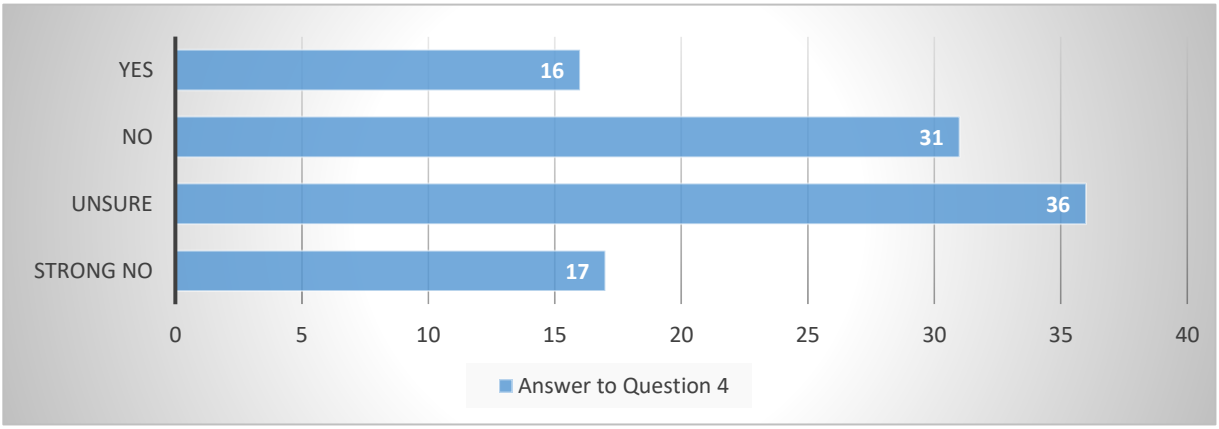


Figure 14: Survey results on trust in the state on privacy, Nigerians under the Adelola et al. (2015) survey.

Discussion. From the results, it is apparent that the long-term lack of privacy laws in Nigeria has put finance institutions' customers to develop a distrust of the government on data. Indeed, apart from the large banks, many upcoming financial institutions in the country are under no privacy laws, while the majority do not enforce the existing ones (Egboro, 2015).

The closest code of privacy was the 'NCC Act of 2007' (DLA Piper, 2017). It stipulates the safe upkeep of customer information in servers and the deletion of the same in due time (DLA Piper, 2017). However, its role does not holistically cover the entire industry for it evolved as an umbrella law for the telecoms (DLA Piper, 2017). For this reason, it is apparent that many locals are not bothered about the information they enter online, as they are not sure whether a privacy law covers them as the foregoing case study has revealed (Adelola, 2015).

Findings on Beck et al. (2011)

The case study by Beck et al. (2011), sought to convey the idea that there was a thin line between what constitutes privacy laws for micro-finance institutions and informal banking outlets. The survey found that in countries like Kenya, 33% of the respondents did not have any financial affiliation, while 26% were in microfinance (Beck et al., 2011). In Malawi, on the other

hand, the majority of the surveyed were informal financial institutions, at 55%, while 19% of the participants were in microfinance. In Namibia, 2% were in microfinance while 52% were unbanked. Uganda had 42% of microfinance respondents while 33% had no financial affiliation. The respondents from Zambia were 14% from microfinance while 65% were unbanked (Beck et al., 2011). Since informal banking outlets have little regulations, it was likely that some microfinance institutions might also fall under the same categorization (Beck et al., 2011).

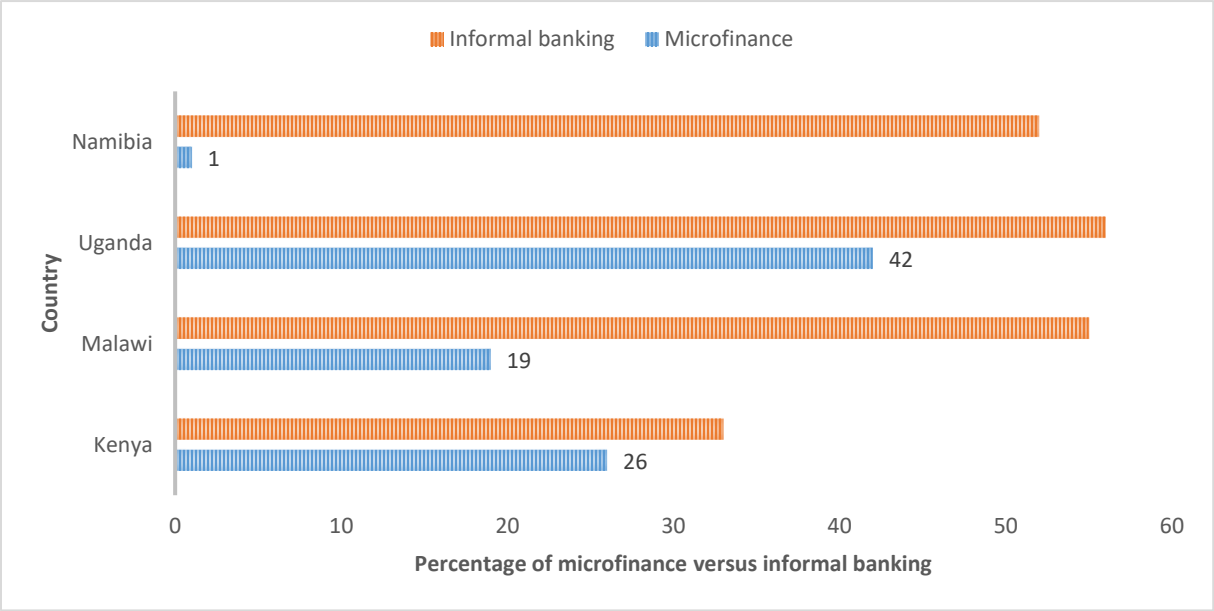


Figure 15: Informal banking vs. microfinance, survey results by Beck et al. (2011).

Discussion. The aspects of privacy and data protection in most Sub-saharan Africa nations borrow partially from an interpretation of telecom, constitutional or other electronic privacy regulations (Jones, 2016). Therefore, with their larger population of users in comparison with their microfinance equivalents, informal banks bring the risk of no direct law to quote about privacy (Beck et al., 2011). In Kenya, for instance, mobile banking, as the most popular informal banking method has technological advances that the local privacy laws have not yet covered

(Malala, 2013). For these reasons, it is clear that the majority of informal banking avenues hurt the adoption of strong data protection regulations in microfinance establishments due to their similarities (Beck et al., 2011).

Findings on Gyabi & Shrivas (2016)

The case study by Gyabi and Shrivas (2016), sought to assess the implementation rate of privacy and data security rules as well as the frequency of their enforcement in Ghanaian rural micro-banks. The first question of "which data privacy policy does your company have?" received the following answers: 36% remarked on recorded policies. 20% remarked of written policies. 11% remarked on data encryption policies. 28% remarked on acceptance policies while 5% highlighted social networking policies (Gyabi & Shrivas, 2016). An acceptance policy is a privacy statement mostly at the bottom of online sites of banks that the user ticks to the effect that he or she consents to a service with or without reading it (Lee, 2016). Under EU data laws, it is now possible to remove consent as easily as accepting it (Lee, 2016). A written policy is meant for reading in full, and the user can retrieve it in a portable format if it is in an electronic database (Lee, 2016). A recorded privacy policy is in audio format. Social networking policies are privacy settings that govern individual preferences including the sharing of data with people by age group (Aldhafferi, Watson, & Sajeev, 2013). Data encryption policies govern the securing of personal data by companies when sending it via electronic format such as via email.

On the question on "which was the last date when your bank updated data breach action guideline?" the results were as follows: 19% reported no update. 46% reported updates in 12 months. Four percent reported an extent of over 5 years without updates. 22% reported updates in 24 months. Nine percent reported updates every 5 years (Gyabi & Shrivas, 2016).

On the question: "does your financial outlet undertake mock information recovery tests to prepare for breaches?" the study recorded these outcomes: 5% did not know. 46% reported a 'Yes.' 49% reported a 'No ' (Gyabi & Shrivas, 2016). The chart below presents the graphical results of this last question:

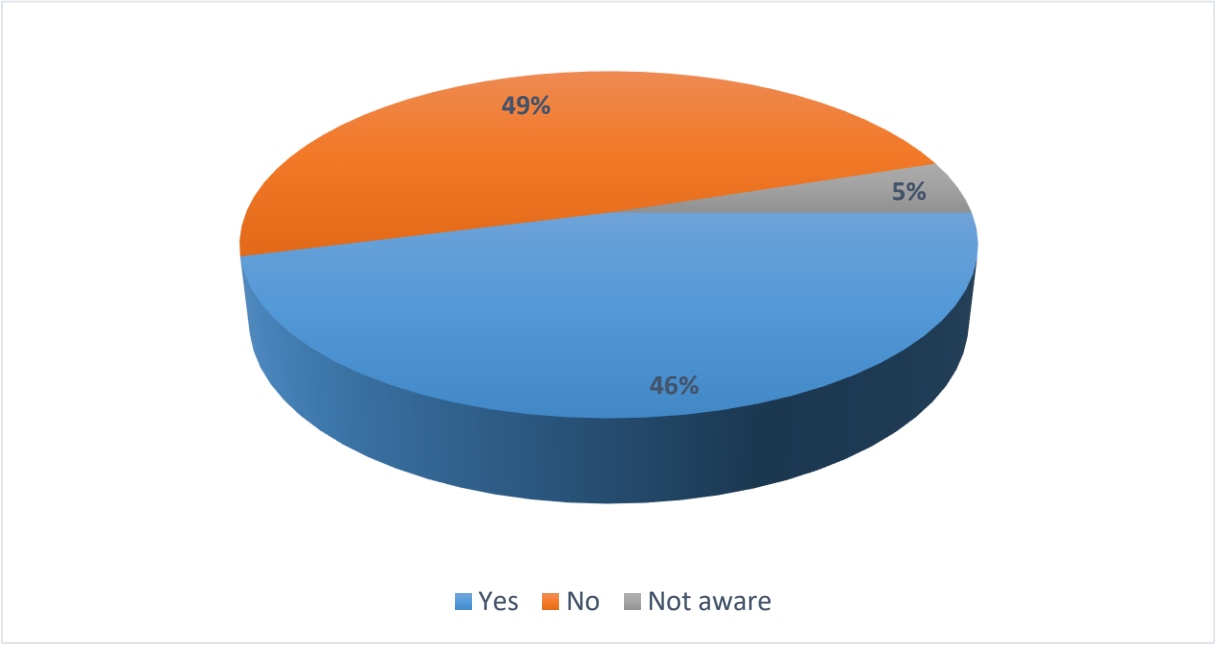


Figure 16: Percentage of frequent data breach mock tests by rural micro-banks in Ghana, Gyabi, and Shrivas (2016).

Discussion. From the data above, it is apparent that 'acceptance' data privacy policies and recorded policies at 28% and 36%, respectively, are higher than written policies, at 20%, data encryption policies, at 11% and social networking policies, at 5% (Gyabi & Srhivas, 2016). It is also apparent that nearly half of the surveyed rural banks do not regularly update their security and data protection policies, manifest in the fact that they rarely test their systems for vulnerabilities (Gyabi & Shrivas, 2016). Micro-finance institutions in Ghana are under the 'Banking Act of the year 2004' (Asante, 2017). Though it deals mainly with financial matters, the clause regulates on many issues, including data privacy. Indeed, many micro-finance institutions

did not pass the test when it first came in the mid-2000s (Asante, 2017). From the fact that the above survey took place four years after the enactment of the newest privacy law in Ghana of 2012 (Dagbanja, 2016), it is apparent that the micro-finance institutions are still in the developing stages.

Findings on Shuhidan et al. (2017)

The findings on the Shuhidan et al. (2017), Malaysia case study on the security of the data of microfinance consumers who used mobile banking was to the effect that:

1. “Are you of the view that your mobile banking data is at risk every time you sign in?”

With a mean score of 3.2, with 5 being the highest score, customers expressed concern that their sensitive data would be accessible in their absence after they had first logged into their accounts (Shuhidan et al., 2017).

2. “Are you of the view that your mobile banking data is at risk of hacking?”

With a mean score of 3.6, where 5 is the highest value, most customers expressed the misgivings that they did not use mobile-based microfinance because their data might be compromised by hackers (Shuhidan et al., 2017).

The results in graphical form are as below:

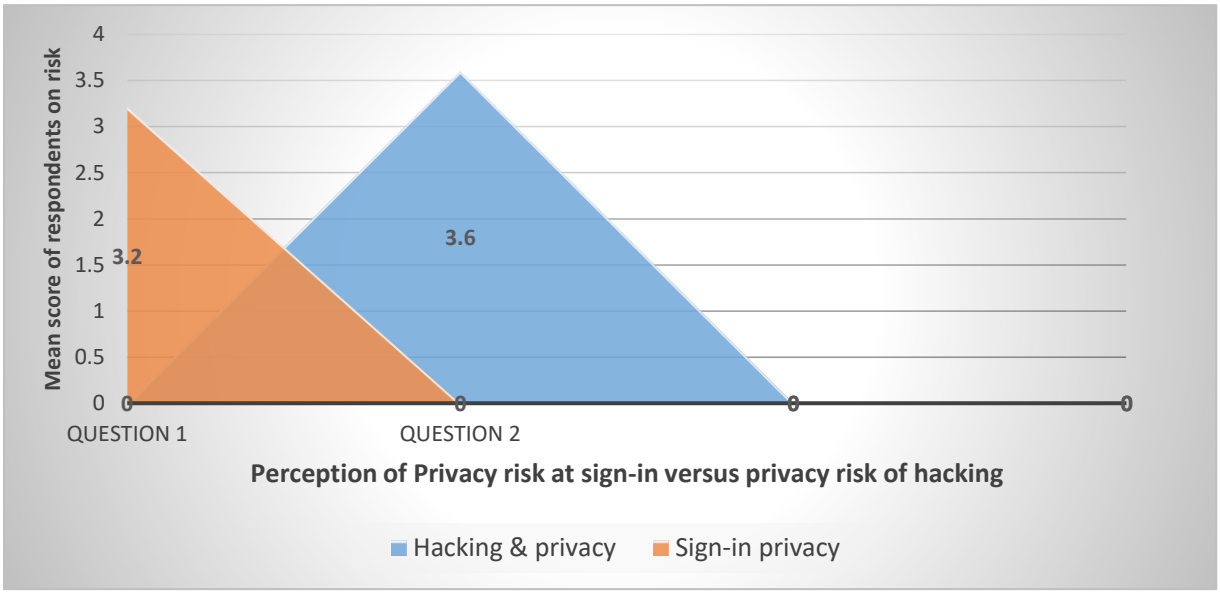


Figure 17: Perception of privacy risk at sign-in vs. privacy risk of hacking.

Discussion. The microfinance sub-sector in Malaysia dates back to the late 1980s to facilitate loan accessibility to the era's unbanked population (Mokhtar, Nartea & Gan, 2012). Up to 2010, Malaysia utilized a 20th-century data law that did not reflect emerging technologies. After the national assembly passed the bill on individual data privacy in 2010, it was a turning point. Before then, even the constitution did not have a direct mention of 'banking privacy,' and so courts used precedents to resolve data breach cases, especially in mobile banking (Cieh, 2013). This legal background may highlight the above case studies results in that many locals are yet to approach the laws seriously fully and they take to privacy in microfinance warily (Cieh, 2013).

Findings on the Variable of Information Security Laws in East Africa/ West Africa Report (2017)

This is about the report by Baur-Yazbeck et al. (2017) that cybercrime in East and West Africa pertains mostly to financial losses via mobile banking data vulnerabilities. As

aforementioned in the methodology section, the variables of cybercrime in these Sub-Saharan Africa regions included identity theft, virus planting and 'social engineering' (Baur-Yazbeck et al., 2017). The results of the report on lax mobile banking in East Africa presented consolidated results across the above three strands of information security (Baur-Yazbeck et al., 2017). In the East African region, Kenya had the highest negative outcomes: poor information security in mobile finance cost the country a hundred and seventy-five million US dollars in 2016 (Baur-Yazbeck et al., 2017). Tanzania followed with eighty-five million US dollars while data breaches in Uganda's micro-banking amounted to thirty-five million US dollars. In West Africa, poor information security regulation cost the micro-banking sector of Nigeria five hundred and fifty US dollars. Appendix F has information on the percentage of cyber crime related to mobile banking using the above Sub-saharan countries' data.

Discussion. To alleviate data breaches associated with its rise as the regional pioneer of mobile banking, Kenya enacted an act in 2010 that embraced the communications sector (Baur-Yazbeck et al., 2017). Uganda, on the other hand, has enacted information security laws that borrow from similar cyber decrees in the economic bloc of East African nations (Baur-Yazbeck et al., 2017). Therefore, from the above financial losses, it is apparent that the laws are not well implemented.

Findings on the Variable of Privacy Laws in Myanmar Survey (2015)

The following are the findings of the case above study in Myanmar in 2015. The case focused on the number of companies, seventy-three in all, which implemented various aspects of privacy policies.

Findings. On the issue of the explicit statement of privacy statements, just 6 of the 23 entities had clear guidelines on clients', employees' and affiliates' information (Myanmar Center for Responsible Business, 2015). Only three had their privacy statements embedded onto their main corporate policies, such as mission and ethics. Regarding exceptions to data privacy, one Information Service Provider had no disclosure on privacy anywhere on its site (Myanmar Center for Responsible Business, 2015). Overall, the bulk of the surveyed entities especially in micro-finance did not parade information on the way they would handle their clients' privacy as the law required of them. The chart below depicts the findings.

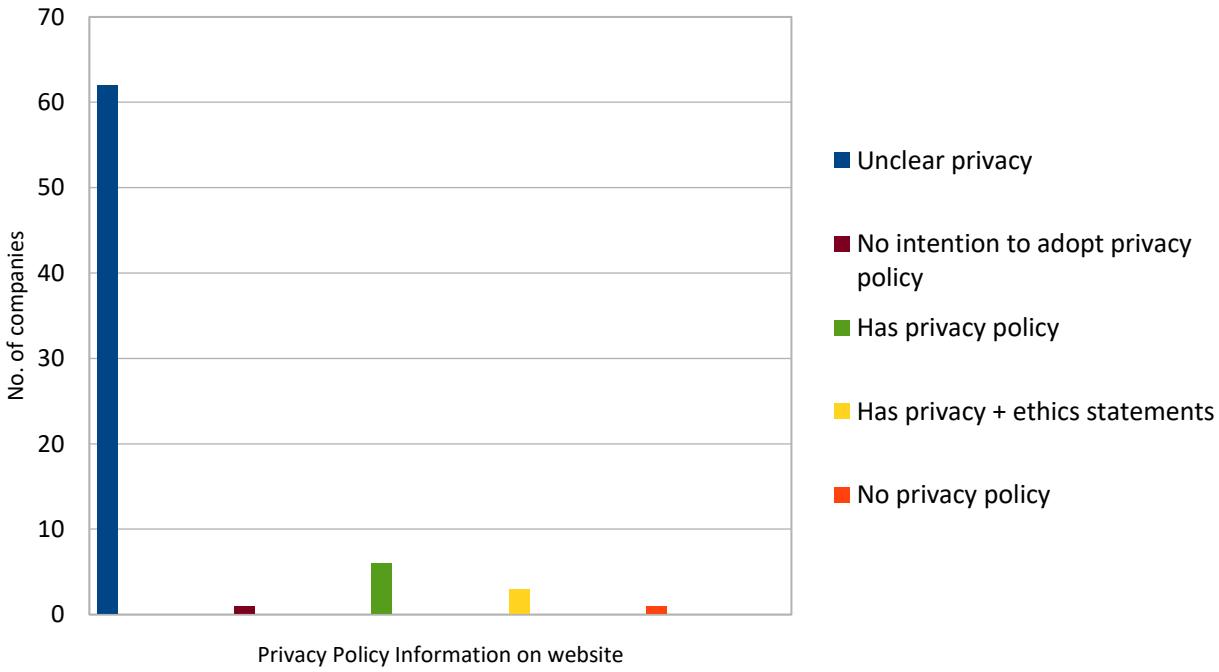


Figure 18: Availability of privacy policy information on website (Myanmar Center for Responsible Business, 2015).

Discussion. In Myanmar, it is illegal by law to misuse the private information of clients of micro-finance establishments (Choudhary, 2017). This is under the first item of the Notifications decree of 2016 (Choudhary, 2017). The clause not only bars the institutions not to

avail sensitive details that are personal to clients but that a search about a customer's state of debt should not dig too deep into the individual's privacy (Choudhary, 2017). For this reason, it is apparent that most micro-banks in Myanmar are not able to even assess the amount of debt a client can afford because of the restrictions (Choudhary, 2017). For this reason, they often rely on other banks that the customer may be privy to for verification purposes (Choudhary, 2017). It is notable that the Notifications Act of 2016 came after the above survey took place and thus had no effect on the outcomes.

Findings on Sun and Lee (2013)

This section concerns the ineffectiveness of data privacy management system by banks in South Korea to keep up with the country's 'Personal Information Protection Law of 2012' (Sun & Lee, 2013). The study suggests that despite the increment in online banking, there is a dearth of an understanding of the most effective privacy management system or database in banking institutions (Sun & Lee, 2013). The authors assert that such a system has been challenging to maintain due to the fast pace of financial software in a technology-savvy country like South Korea (Sun & Lee, 2013). Some of the challenges include the lack of enough resources in private financial outlets to regularly calibrate such a system (Sun & Lee, 2013).

Discussion. It is clear that in Korea, privacy issues in banking emanate from technological advances and powerful privacy laws which banks find it hard to maintain (Yoo, Kang, & Kim, 2015). The 2012 law was a follow-up to the 2006 EFTA law that sought to safeguard information security in finance (Sohn, 2016; Sun & Lee, 2013). In 2017, the sharp rise of financial software in banking saw the country's watchdog on data security highlight that the more users get access to programs, the greater their financial data becomes less private (Yonhap,

2017). Other sources claim that users may even have low motivation in the utility of online banking if technology presents more privacy exposure than it covers (Kim & Chi, 2015).

Data privacy in Korea had existed since 1999 when the 'E-Documents Act' (Sohn, 2016) came to be. In the course of the past 20 years. This act has grown together with the 'EFTA' framework that guides information security in finance (Sohn, 2016). Therefore, despite strong privacy in a developing country, there are still technical vulnerabilities. Appendix I and J have the details of the progress of the data privacy laws timeline in Korea.

Findings on Mommens (2016)

The case in question is a publication in 2016 that stipulated that between 2014 and 2015, Senegal's largest microfinance outlets suffered breaches together with their governmental equivalents from cybercrime. The outcome of the above case study was to the effect that data laws in Senegal, with the latest one being of the year 2008 (Boshe, 2016), have been ineffective as the attacks took place only half a dozen years later. The table below presents the three variables above and their effect on Senegal's 2014 to 2016 micro-finance breaches.

Table 7

Reasons for Data Breaches in Senegal

Reason for privacy and data breach in Senegal's microfinance	Outcome
Weak regulation of privacy and data protection laws	Loss of sensitive client information (Mommens, 2016).
Direct loss of money in accounts	It accounted for 80 percent of all information security breaches of microfinance in the study period (Mommens, 2016).
Low trust by banks on technology	Due to the heightened rate of cyber-attacks, micro-finance institutions have been left behind from developing in tandem with technology (Mommens, 2016).

Discussion. In Senegal, information security and privacy regulation are composite of 'Law Number 2008 to 2012' (Privacy International, 2013). The clause covers a range of data borderlines including that between users of mobile devices and banking data. The closest it comes to microfinance is the stipulation for financial and mobile service providers to uphold individuals' data and not transmit it to affiliates without the owner's consent (Privacy International, 2013). Applying these laws to the outcomes of 2014 to 2016, it is apparent that there were loopholes for the country as the breaches happened even in the existence of the cybercrime 'Law Number 2008-2011' (Privacy International, 2013). As a proof of their

ineffectiveness, the 2014-2016 attacks took place just a few years after the laws (Mommens, 2016; Boshe, 2016).

The Conclusion to Findings and Discussion

Of the ten case studies, apart from Malaysia and Nigeria all other developing countries show a low presence of privacy regulations, while all four developing countries studied shows high to medium presence of privacy regulations. Whereas, level of enforcement of privacy regulations and level of effectiveness of privacy regulations, the other two factors discussed all has a clear differential between developed and developing countries with only Malaysia as a developing country has a medium level of enforcement and effectiveness in privacy regulations (see Appendix H).

The Federal Trade Commission (2015), and the Securities Exchange Commission (2016), case studies present mixed outcomes for the 2012-2014 Morgan Stanley data breach in the US. Adeola et al. (2015), show the failure of the application of privacy laws in Nigeria's micro-finance sector. The same applies to Shuhidan et al. (2017), in their survey on Malaysia where customers distrust signing in for fear of data misuse. Gyabi and Shrivas (2016), also reveal a failure in the privacy protection mandate in Ghana's rural banking. In Burma, the Myanmar Center for Responsible Business (2015), reports that just three out of seventy-three entities have clear on-site guidelines on the privacy of the users and affiliates. Mendel et al. (2012), also show that breaches still happen in a developed country, namely South Korea. The study has also documented failure in Senegal from a cybercrime spree of 2012 to 2014 (Mommens, 2016).

Regarding the variable of the presence of privacy regulations, it is apparent that most countries within developing countries have no sufficient data protection measures. For instance,

Kenya and Nigeria have both lost millions of dollars through mobile banking crimes (Baur-Yazbeck et al., 2017). Regarding the variable of the presence of privacy regulations, it is clear that developing countries have outdated policies that do not reflect modern technology and thus most consumers are not aware of the laws. In developed nations, privacy laws are quite clear, for instance in the European Union, but still, breaches happen such as the Snowden leaks (Kuner, 2014).

Table 8

Variables of the Research (Results in Appendix H).

Variables	**Evaluation**
Presence of privacy regulations	Low/Medium/High
Level of Enforcement of privacy regulations	Low/Medium/High
The effectiveness of privacy regulations	Low/Medium/High

Presence of privacy regulations and enforcement of privacy regulation both affect the effectiveness of those privacy regulations. The findings reveal that the level of effectiveness of the privacy and data protection legislation in developing countries is ineffective to keep up with modern technologies. Those of the developed countries, on the other hand, are strong but require regular updates.

From the above evaluation, the consensus is to the effect that data security is still in a developing stage in the Third World while its level of embracement in the developed countries revolves around the maximum level of implementation. For instance, the findings in the South Korea data breach of 2011 reveal that in the case where 90 percent of the web users were affected by a data breach, the reason was extra-strong SSN enforcement (Mendel et al., 2012).

Therefore, extra precautionary measures may misfire when the hackers' technology gets access to the most sensitive SSN information of the users (Mendel et al., 2012). This is despite the laws in Korea being up-to-date.

In Malaysia's ongoing modernization of privacy laws, the ramifications of waiting too long between the 1990s and the current decade have seen many consumers fear that signing in leaves their data open to misuse (Shuhidan et al., 2017). Indeed, it is one of the states in the developing world with the recent impressive growth of privacy laws. The latest legislation reflects a country eager to align its privacy protocols with those of the European Union and the regional south-east Asia economic bloc (Yu, 2014).

In Africa, the findings reveal the lack of awareness by the customers due to the deficiency of information on their online privacy, especially about online eCommerce and micro-finance (Adelola et al., 2015). For instance, the results from Nigeria have shown that just 20% of financial services' users in a survey are concerned about what they input online while 44% are concerned only on occasion (Adelola et al., 2015). This is even though the West African nation perpetually reigns in on banks and micro-finance institutions with new laws, the latest one being in 2010 (Makulilo, 2012).

In short, there is a disparity between the developed privacy laws of Western countries that make financial firms accountable for privacy compromises (Securities & Exchange Commission, 2016) and those of developing nations. The laws of the latter either exist only generally in the constitution, are in draft format or are behind technology (Makulilo, 2012; Privacy International, 2016).

Chapter 5: Conclusion

In summation, three glaring elements define privacy and data regulations worldwide. The first one is the imitation of the general data protection regulations of the European Union in developed nations. The second is the slow drafting of new laws in developing countries. The third one is the exposure of consumer privacy to hackers and social engineering breaches, especially in micro-finance institutions (Baur-Yazbeck et al., 2017).

About the first point, the European Union's new framework that governs online data breaches is set to overrule those of member states in mid-2017. Cross-border data leaks have made many countries see the need for EU-like regulations that are 'international' (Kuner, 2014). The legal conundrum surrounding whether to adopt similar regulations is that they are quite strong for nations outside the EU as even local businesses are yet to prepare for them (Gordon, 2017). Nevertheless, the lack of improvisation of similar policies may hurt trade relations where data breaches may lead to misunderstandings. The United States, for this reason, is still deliberating whether to forge stringent rules like those on the other side of the Atlantic (Movius & Krup, 2009).

In respect to the second point of slow privacy and data law development in developing countries, the study has shown that there are exceptions but these are few. For instance, Malaysia is under a renaissance of its 1990s laws with an ongoing stance towards EU-affiliated policies (Yu, 2014). In South America, despite the common use of electronic payment systems, Brazil was still indecisive on the promulgation of cyber laws to govern the cards by 2014 (Johnson et al., 2014). Most Asian nations are still relying on their cyber protection laws of the 1990s that do not bear on the changing technology (Greenleaf, 2014). The majority of Sub-Saharan African

states still have underdeveloped micro-finance data laws: for instance in Uganda; the laws are yet to exist although the majority of the population relies on the micro institutions for their banking needs (Mwesigwa, 2010).

On the point of data exposure by both financial and micro-finance institutions, the study has shown that the effect is prevalent in the developing countries. Worthy mentions include Kenya, Nigeria, and Ghana, which are some of the countries in Africa with the highest rates of micro-finance cybercrime (Baur-Yazbeck et al., 2017). In Kenya, for instance, lax mobile banking information security cost the country $175 million in 2016 (Baur-Yazbeck et al., 2017). However, when a breach happens in a developed nation, it is usually of high impact. For instance, the South Korea hacking of 2011 left thirty-five million dependents of the country's Internet affected. In the United States, on the other hand, a worker at Morgan Stanley left over seven hundred and thirty thousand clients' files up for sale online despite the strong measures the firm put as a safeguard (Federal Trade Commission, 2015).

In short, if the current privacy law in Europe comes to affect other states, it may lead to fewer cases of data breaches in states that implement it (Hert & Papakonstantinou, 2013). However, if developing nations stay put with outdated systems, technological breakthroughs by hackers will force the countries to improvise new laws (Hert & Papakonstantinou, 2013). In the current context, it is apparent that few financial companies in, especially, developing nations fully enforce privacy laws.

Limitations

During the evaluation of research material for this work, the study encountered the lack of sufficient information that directly applied to the subject of privacy information in the context

of micro-finance and finance. The majority of the research literature hinged upon privacy and data protection in a general context. Another limitation was an unclear separation between micro-finance and informal banking, especially in the context of information security in developing countries. While some nations have data privacy laws specifically for microfinance, the legislation are often overshadowed by those for mobile banking which has the majority of users. A final and significant limitation was the fact that legislation in microfinance in most databases was of a credit regulation nature as opposed to data protection and privacy. Much of the gist of the legal framework aims to buffer consumers against financial exploitation by the micro-banks but not on privacy. To overcome these limitations, there was the necessity for thorough research of only case studies that were relevant to the study.

Future Work

In trying to answer one of the major discrepancies of this research, namely consumers' lack of awareness in privacy issues, especially in developing nations, future research can dwell on privacy and data protection education (Dennis, 2011). Certain third world countries like the Philippines are having such literacy drives (Dennis, 2011). This will alleviate the tendency by microfinance institutions in places like Lebanon and Nigeria to informally disburse client information to affiliates or openly discuss consumer data openly irrespective of privacy restrictions for such behavior in the respective countries (Abbassi, Khaled, & Lauer, 2009; Egboro, 2015). When consumers learn their privacy rights, they will not warrant their confidential to become a discussion point in boardrooms (Egboro, 2015).

The coming of the General Data Protection Regulation in Europe in mid-May 2018 will also have an educational impact on countries outside the European Union that wish to follow it.

This is because they will need to educate their consumers about the rules when they adopt them just like European companies are preparing for the rules (Gordon, 2017). Thus, there is a need to research further on the aspect of consumer awareness of privacy laws through education.

References

Abdulrauf, L. A. (2016). *The legal protection of data privacy in Nigeria: Lessons from Canada and South Africa.* Pretoria: University of Pretoria.

Adelola, T., Dawson, R., & Batmaz, F. (2015). *Nigerians' perceptions of personal data protection and privacy.* SQM Conference 2015.

Agelidis, Y. (2016). Protecting the good, the bad, and the ugly: 'Exposure' data breaches and suggestions for coping with them. *Berkeley Technology Law Journal, 31*(2).

Aldhafferi, N., Watson, C., & Sajeev, A. S. M. (2013). Personal information privacy settings of online social networks and their suitability for mobile internet devices. *International Journal of Security, Privacy and Trust Management, 2*(2).

Allen, & Overy LLP. (2017). *The EU general data protection regulations 2017* (pp. 2-48). London: Allen & Overy LLP.

Ardic, O. P., Ibrahim, J. A., & Mylenko, N. (2011). *Consumer protection laws and regulations in deposit and loan services: a cross-country analysis with a new data set.* Washington, DC: World Bank.

Arun, T., & Murinde, V. (2010). *Microfinance regulation and social protection.* Brussels: European Report on Development.

Asante, E. K. (2017). *Competitive strategies of microfinance owners in Ghana.* Minneapolis, MN: Walden University.

Baker, L. (2016). Protection regulation on the banking sector: Data subjects' rights, conflicts of laws and Brexit. *Journal of Data Protection & Privacy, 1*(2), 137-145.

Baur-Yazbeck, J. I., & Valenzuela, M. (2017). *Emerging trends in Sub-saharan Africa: Policymakers' perspectives.* Washington, DC: World Bank/CGAP.

Blum, D. (2017). Digital identity-will the new oil create fuel or fire in today's economy? *ISACA Journal, 6.*

Booysen, S. & Neo, D. (2017). *Can banks still keep a secret?* Cambridge: Cambridge University Press.

Boshe, P. (2016). Protection of personal data in Senegal. *African Data Privacy Laws,* pp 259-275.

Brink, S. T., Wang, J., Veldhoen, D., & Arnbak, A. (2017). China's new cybersecurity law-effective as of 1 June 2017. *Trade Security Journal, 2,* 27-29.

Broadhurst, R. G., & Chang, L. Y. C. (2013). Cybercrime in Asia: trends and challenges. SSRN Electronic Journal. In *Handbook of Asian criminology* (1st ed., pp. 49-63). New York: Springer.

Brodie, N. (2014). *How does cybercrime affect you?* Retrieved on March 21, 2018, from https://www.mh.co.za/guy-skills/how-does-cybercrime-affect-you/.

Budnitz, M. E. (2016). *The legal framework of mobile payments: Gaps, ambiguities, and overlap.* Philadelphia, PA: The Pew Charitable Trusts.

Bu-Pasha, S. (2017). Cross-border issues under EU data protection law with regards to personal data protection. *Information & Communications Technology Law, 2017,* pp 213-228.

Camillo, M. (2016). Cybersecurity: Risks and management of risks for global banks and financial institutions. *Journal of Risk Management in Financial Institutions, 10*(2), 196-200.

Cano, M. J. J. (2014). The information security function: Current and emerging pressures from information security. *ISACA Journal, 6.*

Carbo-Valverde, S. (2016). The impact on digitalization on banking and financial stability. *Journal of Financial Management Markets and Institutions, 5*(1), 133-140.

Carey, G., & Silva, P. (2016). *Bill of law which will modify the Chilean data privacy act: Comments to the minutes sent by the Ministry of Finance to the Congress.* Retrieved on March 12, 2018, from http://www.mondaq.com/x/499782/Data+Protection+Privacy/Bill+Of+Law+Which+Will+Modify+The+Chilean+Data+Privacy+Act+Comments+To+The+Minutes+Sent+By+The+Ministry+Of+Finance+To+The+Congress.

Cassim, F. (2015). Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves? *P.E.R., 18*(2).

Cieh, E. L. Y. (2013). Personal data protection and privacy law in Malaysia. From the book: *Beyond data protection: strategic case studies and practical guidance,* pp 5-29.

Charlesworth, A., & Stanton, K. (2016, November 11). *Tesco Bank and Cybercrime.* Retrieved on March 15, 2018,.from Tesco Bank and Cybercrime: https://legalresearch.blogs.bris.ac.uk/2016/11/tesco-bank-and-cybercrime/.

Choudhary, N. (2017). *Myanmar-microfinance institutions and their obligations under the 2016 notifications.* Retrieved on March 17, 2018, from http://www.inhousecommunity.com/article/myanmar-microfinance-institutions-obligations-2016-notifications/.

Clarke, H. (2016, December 8). *Bold cyber security regulations for the financial services industry–will we see them in australia?* Retrieved on March 01, 2018 from http://www.

corrs.com.au/thinking/insights/bold-cyber-security-regulations-for-the-financial-services-industry-will-we-see-them-in-australia/.

Craig, C., Jansen, T., Eecke, P. V., Umhoefer, C., Shaik, R. V., Christie, A., & Halpert, J. (2013). *Data protection laws of the world*. DLA Piper.

Dagbanja, D. N. (2016). the right to privacy and data protection in Ghana. *African Data Privacy Laws,* pp. 229-448.

Dahiru, A. A., Bass, J. M., & Allison, I. (2014). Cloud computing: Adoption issues for Sub-saharan African SMEs. *Electronic Journal of Information Systems in Developing Countries, 62*(1), 1-17.

Davis, D. (2018, April). *GDPR: An overview of the latest data protection legislation.* Retrieved on March 21, 2018, from https://www.computerweekly.com/feature/GDPR-An-overview-of-the-latest-data-protection-legislation.

Directo, A. D. (2014). Data protection in India: The legislation of self-regulation. *Northwestern Journal of International Law & Business, 35(1).*

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. *Computer & Security, 30,* 1-10.

DLA Piper. (2017). *Data protection laws of the world: Nigeria.* London: DLA Piper.

Egboro, E. M. (2015). Creation of microfinance banks in Nigeria: What is their main object? *British Journal of Economics, Management & Trade, 7*(3), 158-174.

European Union Agency for Network and Information Security (Enisa). (2014). *Network and information security in the finance sector.* Brussels: European Union Agency for Network and Information Security.

Ezeoha, A. E. (2006). Regulating internet banking in Nigeria: Some success prescriptions-Part 2. *Journal of Internet Banking and Commerce, 2006, 11*(1).

Federal Trade Commission. (2015). *Closing letters Morgan Stanley.* Washington, DC: Federal Trade Commission.

Fotabong, L. A. (2012). *The microfinance market of Cameroon: Analyzing trends and current developments.* Doula: Fotabright Market Insights.

Frost, E. (2017, February 1). *Hacking Tesco Bank: The changing nature of bank robbery*. Retrieved on March 01, 2018, from https://internationalbanker.com/banking/hacking-tesco-bank-changing-nature-bank-robbery/.

Gordon, S. (2017). *Businesses failing to prepare for EU rules on data protection.* Retrieved on March 17, 2018, from https://www.ft.com/content/28f4eff8-51bf-11e7-a1f2-db19572361bb.

The Government of the Philippines. (2014). *Senate bill no. 2965 Data Privacy Act of 2011.* Manila: Author.

Greenleaf, G. (2014). *Data privacy laws in Asia-context and history.* Oxford: OUP.

Gyabi, M. O., & Shrivas, M. K. (2016). Data security in the rural banking sector: A case study in Ashanti region. *International Journal of Advanced Research in Computer Science & Technology, 4*(2), 99-106.

Hamidovic, H. (2014) Electronic documents information security compliance. *ISACA Journal, 3.*

Hert, P. D., & Papakonstantinou, V. (2013). Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN agency? *I/S: A Journal of Law and policy For the Information Society, 9*(2), 273-324.

Jamil, D., & Khan, M. N. A. (2011). Data Protection Act in India compared to the European Union countries. *International Journal of Electrical & Computer Sciences IJECS-IJENS, 11*(06), 16-20.

Johnson, J., Lincke, S., Imhof, R., & Lim, C. (2014). A comparison of international information security regulations. *Interdisciplinary Journal of Information, Knowledge, and Management, 9,* 89-116.

Jones, R. (2016, December 1). *Tesco Bank cyber attack involved guesswork, study claims*. Retrieved on February 12, 2018, from https://www.theguardian.com/technology/2016/dec/02/tesco-bank-cyber-attack-involved-simply-guessing-details-study-claims.

Kabanda, S. K. (2010). South African banks and their online privacy policy statements a content analysis. *Journal of Information Management*, *12*(1).

Kenyon, A. T. (2016). *Comparative defamation and privacy law.* Cambridge: Cambridge University Press.

Kershaw, R. (2014). *A catch-22 in Asian eDiscovery.* Retrieved on March 12, 2018, from http://www.ftijournal.com/article/a-catch-22-in-asian-ediscovery.

Khan, M. J. (2016). Managing data protection and cybersecurity audits role. *ISACA Journal, 1.*

King, N. J. (2008). Direct marketing, mobile phones, and consumer privacy: Ensuring adequate disclosure and consent mechanisms for emerging mobile advertising practices. *Federal Communications Law Journal, 60*(2), 229-324.

Klimburg, A., & Zylberberg, H. (2015). Cybersecurity capacity building: Developing access. *Norwegian Institute of International Affairs, NUPI Report No. 6, 2015.*

KPMG. (2017). *Overview of China's cybersecurity law.* Beijing: KPMG China.

Kuner, C. (2014). The European Union and the search for an international data protection framework. *Groningen Journal of International Law, 2*(1).

Lane, J. (2014). The internationalism of information privacy: Towards common protection. *GroJIL, 2*(2), 115-144.

Laube, S., & Bohme, R. (2016). The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity, 2*(1), 29-41.

Lee, P. (2016). *The nuance of 'accepting' vs. 'reading' a privacy policy.* Retrieved on March 21, 2018, from http://privacylawblog.fieldfisher.com/2016/the-nuance-of-accepting-vs-reading-a-privacy-policy/.

Lumsden, E. (2013). Securing mobile technology & financial transactions in the United States. *Berkeley Business Law Journal, 9*(1).

Maimbo, S. M., Faye, I., & Triki, T. (2011). *Financing Africa: Through the crisis and beyond.* Washington, DC: World Bank Publications.

Makulilo, A. B. (2012). Nigeria's data protection bill: Too many surprises. *Privacy & Business, 120,* 25-27.

Makulilo, A. B., & Mophethe, K. (2016). Privacy and data protection in Lesotho. *African Data Privacy Laws,* pp 337-347.

Mello, L. A. (2012). Tax competition and the case of bank secrecy rules new trends in international tax law. *SGD Dissertations, Paper 1.*

Mendel, T., Puddephatt, A., Wagner, B., Hawtin, D., & Torres, N. (2012). *Global survey on internet privacy and freedom of expression.* Paris: UNESCO Series on Internet Freedom.

Miskam, S., & Shahwahid, F. (2014). *Privacy and personal data protection the legal framework in Malaysia and its implication in the financial service sector.* Seminar Teknologi Maklumat & Masyarakat, 2014.

Mohammed, D. (2015). Cybersecurity compliance in the financial sector. *Journal of Internet Banking and Commerce (JIBC), 20*(1).

Mokhtar, S. H., Nartea, G. & Gan, C. (2012). The Malaysian microfinance system and a comparison with the Grameen Bank (Bangladesh) and Bank Perkreditan Rakyat (BPR-Indonesia). *Journal of Arts and Humanities (JAH), 1*(3), 60-71.

Mommens, X. (2016). The importance of cyber security for digital finance. *European Microfinance Week 2016.*

Movius, L. B., & Krup, N. (2009). U.S. and EU privacy policy: Comparison of regulatory approaches. *International Journal of Communication, 3,* 169-187.

Mtuze, S. L. S. (2015). *A comparative review of legislative reform of electronic contract formation in South Africa.* Pretoria: University of South Africa.

Mwafise, A. M., & Stapleton, L. (2012). *Determinants of user adoption of mobile electronic payment systems for microfinance institutions in developing countries: Case study Cameroon.* Waterford: Waterford Institute of Technology, Ireland.

Mwesigwa, R. (2010). *Consumers' attitudes, perceived risk, trust and internet banking adoption in Uganda.* Kampala: Makerere University.

Myanmar Center for Responsible Business. (2015). *Chapter 4.3: Privacy.* Yangon: Author Myanmar Center for Responsible Business, pp 152-164.

Naude (2014). *Data protection in South Africa: The impact of the protection of personal information act and recent international developments.* Pretoria: University of Pretoria.

Ngcamu, B. S. (2016). An empirical investigation into the information management systems at a South African financial institution. *Banks and Bank Systems, 11*(3), 56-63.

Oluyombo, O. O. (2007). Developing microfinance banking in Nigeria. *Babcock Journal of Management and Social Sciences, 6*(1), 126-134.

Omarini, A. (2011). Retail banking: The challenge of getting customer intimate. *Bank and Bank Systems, 6*(3).

Palfrey, M. (2013, December 18). *Australia: AAPT hacking case study.* Retrieved from Mondaq.com:http://www.mondaq.com/australia/x/281166/Data+Protection+Privacy/AAPT+hacking+case+study+what+would+happen+if+it+was+an+agency+under+the+new+law.

Palupy, H. E. (2011). *Privacy and data protection: Indonesia legal framework.* Tilburg: Tilburg University.

Patel, N. (2008). Outsourcing: Data security and privacy issues in India. *Issues in Information Systems, 9*(2), 14-20.

Patricia, C. N., & Izuchukwu, C..D. (2014). The relationship between regulatory inconsistencies and Nigerian banking industry. *Global Journal of Management and Business Research: C Finance, 14*(4).

Pham, L. T. P., Galic, M., & Taylor, L. E. M. (2017). *The European Commission on WIFI4EU: an out-of-service?* Tilburg: Tilburg Law School.

Pouchous, A. (2012). *The regulation and supervision of microfinance: Main issues and progress.* Winnipeg: International Institute for Sustainable Development.

Privacy International (PI). (2016). The right to privacy in Uganda. *Stakeholder Report Universal Periodic 26th Session-Uganda,* pp 1-14.

Raul, A. S. (2014) The privacy, data protection, and cybersecurity law review. *Law Review* (1st ed.).

Sahu, A. (2018). *Philippines: Privacy of client data.* Retrieved on March 11, 2018, from http://www.centerforfinancialinclusion.org/publications-a-resources/client-protection-library/437-philippines-privacy-of-client-data.

Sarabi, A., Naghizadeh, P., Liu, Y., & Liu, M. (2016). Risky business: Fine-grained data breach prediction using business profiles. *Journal of Cybersecurity, 2*(1), 5-28.

Sheng, X., & Cranor, L..F. (2012). An evaluation of the effect of US financial privacy legislation through the analysis of privacy policies. *I/S: A Journal of Law and Policy, 2*(3), 943-979.

Shuhidan, S. M., Hamidi, S. R., & Saleh, I. S. (2017). Perceived risk towards mobile banking: A case study of Malaysia young adulthood. In*ternational Research andInnovation Summit, 226* (2017).

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information security management (ISM) practices: Lessons from select cases from India and Germany. *Global Journal of Flexible Systems Management, 14 I*(4), 225-239.

Srinivas, B. V. (2015, June 15). A concise guide to various Australian Laws related to privacy and cybersecurity.

Sohn, K. H. (2016). Privacy and security protection under Korean e-commerce law and proposal for its improvements. *Arizona Journal of International & Comparative Law, 33*(1), 230-248.

Sorensen, E. J .B. (2017). Data protection poses challenges to the public international law. *International Journal of Public Law, 2017.*

Stander, A., Dunnet, A., & Rizzo, J. (2008). A survey of computer crime and security in South Africa. Cape Town: University of Cape Town.

Solove, D. J. (2006). A brief history of information privacy law. *Prosckauer on Privacy, PLI,* pp 1-46.

Schmidt, D. C., & White, J. (2017). Why don't big companies keep their computer systems up-to-date? Retrieved on March 21, 2018, from http://theconversation.com/why-dont-big-companies-keep-their-computer-systems-up-to-date-84250.

Tse, W. K. D., Hui, M .H., Lam, S. T., Mok, Y. C., Oei, W. C., Tang, K. L., & Yau, X. L. (2013). Education in IT security: a case study in the banking industry. *GSTF Journal on Computing (JoC), 3*(3).

United Nations Conference on Trade and Development (UNCTAD). (2016). *Data protection regulations and international data flow.* Geneva: United Nations Conference on Trade and Development (UNCTAD).

U.S. Securities and Exchange Commission. (2016). *SEC Morgan Stanley failed to safeguard customer data.* Retrieved on March 15, 2018, from https://www.sec.gov/news/pressrelease/2016-112.html.

VanWasshnova, M. R. (2008). Data protection conflicts between the United States and the European Union in the war on terror: Lessons learned from the existing system of financial information exchange. *Case W. Res. J. INT'L L., 39*(3), 827-865.

Vovk, A. (2016, December 1). *Tesco Bank data breach: What went wrong?* Retrieved from https://blog.netwrix.com/2016/12/01/tesco-bank-data-breach-what-went-wrong/.

Walrath, D. (2017). Privacy and information disclosure: An economic analysis of the Gramm-Leach-Bliley Act. *Policy Perspectives, 24,* 55-65.

Yu, W. E. (2014). Data privacy and big data-compliance issues and considerations. *ISACA Journal, 3.*

Zahoor, Z., Ud-din, M., & Sunami, K. (2016). Challenges in privacy and security in the banking sector and related countermeasures. *International Journal of Computer Applications, 144*(3), 24-35.

Appendix A: FTC Ruling on Morgan Stanley Breach of Customer Privacy Through Exposure of Sensitive Data Online (FTC, 2015)

Morgan Stanley Violation	**FTC Ruling**
Information security breach of customer's data.	The bank had implemented the necessary steps to prevent a data breach, so the case was an isolated one.
Exposure to consumer privacy.	The bank was not liable for the individual worker breach as it had prohibited workers' entry into highly protected data repositories and so this was an isolated case.
Lack of system security to reduce data breach.	The bank had a well-maintained cyber-security network. The case applied only to a minor file repository which the company repaired immediately after the breach.

Appendix B: Survey on Privacy View of Users of Nigeria's Financial Institutions by Adelola et al. (2015)

Question	Response
Do you ever get concerned about the data you offer online?	44% said only occasionally.
Have spam messages from non-affiliates to your bank ever keep you on the alert on your data?	38% said they are on the alert all the time while 37% said only on occasion.
Are you knowledgeable of identity theft and its consequences?	4% said they were unaware while 75 percent said they were aware.
Is the state reliable as a custodian of privacy of individual information?	36% were undecided, 31% said no while 16% said yes.

Appendix C: Privacy Questions to Malaysian Mobile Bankers on the Security of Their Data Online

Questions relating to privacy	**Answer**
How do you feel about your private information being used by mobile banks?	
Are you of the view that your mobile banking data is at risk of hacking?	

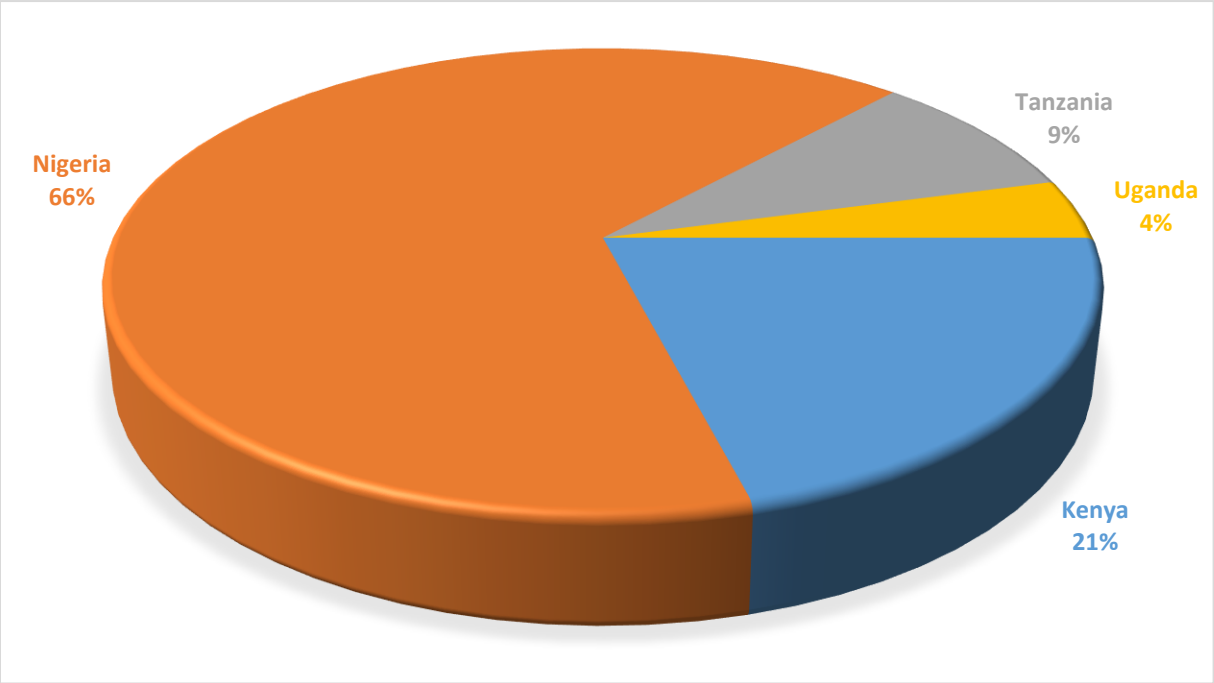
Appendix D: Gyabi & Shrivas (2016) Study on Ghana Micro-banking in Rural Ashanti Recorded the Following Questionnaire Data

Question	Results
Which kind of data privacy policy does your company have?	36 percent remarked on recorded policies. 20% remarked of written policies. 11 percent remarked on data encryption policies. 28 percent remarked on acceptance policies while 5 percent highlighted social networking policies.
1. Which was the last date when your bank updated data breach action guideline?	19% reported no update. 46% reported updates in 12 months. 4% reported above five years without updates. 22% reported updates in 24 months.
Does your financial outlet undertake mock information recovery tests to prepare for breaches?	5% did not know. 46% reported a 'Yes.' 49% reported a 'No.'
If your financial outlet undertakes mock information recovery tests, how often does this happen?	19% remarked no update ever. 46% remarked updates in 12 months. 4% remarked above five years updates. 22% remarked updates in 24 months.

Appendix E: The Financial Dffect of Lax Regulations in Microfinance (Mobile Banking) in East Africa and West Africa

Effect of poor laws on mobile banking in Africa	Kenya in US$	Uganda in US$	Tanzania US$	Nigeria US$
Cybercrime (Virus, malware, identity theft, social engineering)	175 million	35 million	85 million	550 million

Appendix F: Level of Cyber Crime Related to Lax Information Security in Mobile Banking in 2016 by Baur-Yazbeck et al. (2017)



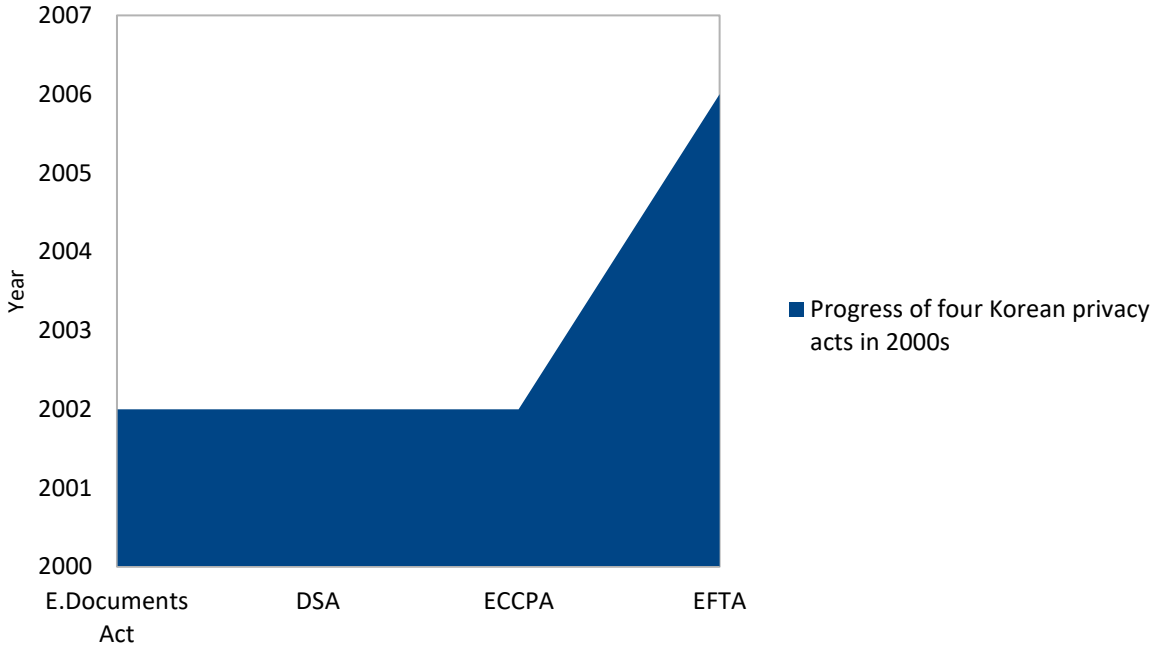
Appendix G: Implementation of Privacy Regulations on Websites in Myanmar in 2014

Privacy Survey model question	**Total: N=73**
Did the companies have in place an explicit privacy statement or data on how they would handle their clients' and stakeholders' information?	6
How many of the 73 entities had their privacy statements embedded as part and parcel of the corporate ethics and mission statement?	3
How many of the 73 companies had put into place sufficient information that a survey could access and interpret about data protection?	Majority
How many entities of the seventy-three had not implemented any privacy regulations on their sites?	1

Appendix H: Empirical Results of the 10 Case Studies. The Summary of Success or Failure Empirical Results of Privacy and Information Security Laws Effectiveness From Different Countries in the 10 Case Studies

Country/Case study	Presence of Security/Privacy Regulations (Low/Medium/High)	Level of Enforcement of Privacy Low/Medium/High)	Effectiveness of privacy Reg. (as per the Researchers)
United States	High	High	Medium
United Kingdom	High	High	High
Australia	Medium	High	Medium
South Korea	Medium	Medium	Medium
Nigeria	Medium	Low	Low
Kenya, Malawi, Namibia, Zambia	Low	Low	Low
Malaysia	Medium	Medium	Medium
Ghana	Low	Low	Low
Uganda, Tanzania	Low	Low	Low
Myanmar	Low	Low	Low
Senegal	Low	Low	Low

Appendix I: The Progress of Four Korean Privacy Laws in the Early to mid-2000s



Appendix J: The Timeline of Privacy Laws Related to Finance in Korea Since 1999

Korea Privacy Law	**Purpose**
E-Documents Act of 1999	Privacy and data security online (Sohn, 2016).
DSA of 2002	For digital signature authorization online especially in finance (Sohn, 2016).
ECCPA of 2002	Privacy of consumers online in e-Commerce, banking and other industries (Sohn, 2016).
EFTA of 2006	For information security in finance (Sohn, 2016).