access to insurance initiative

IAIS
INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

Report of the 19th A2ii – IAIS Consultation Call

Data protection challenges in mobile insurance

24 November 2016

The A2ii consultation calls are organised in partnership with the IAIS to provide supervisors with a platform to exchange experiences and lessons learnt in expanding access to insurance.

The 19th Consultation Call, held on 24 November 2016, focused on exploring data protection challenges arising from mobile insurance business models. Four calls were held: two in English, one in French and one in Spanish.

Technical experts Dr Nicola Jentzsch (Consultant) and Andrea Camargo (Director of Regulation and Consumer Protection at the Microinsurance Catastrophe Risk Organisation, MiCRO) explored important privacy and data protection risks introduced by applying Big Data analytics to the provisioning of insurance, as well as corresponding regulatory considerations for supervisors. Country experts Eugene Du Toit from the South African Financial Services Board and Ranferi Gómez from the Mexican National Commission of Insurance and Finance shared their jurisdictions' experience with data protection in mobile insurance.

Introduction to Mobile Insurance

Mobile insurance, or the provisioning of insurance products through the mobile phone ecosystem, has been rapidly expanding around the world. As of June 2015, the mobile insurance industry featured 120 live services with 31 million active policies in 33 emerging markets[1] . The proliferation of mobile insurance, not only in terms of the scale but also scope of coverage, has made it a strong and growing market with a potentially huge impact.

Mobile Trends within the Microinsurance Market

The microinsurance industry has been steadily growing over the past few years. The first comprehensive stocktaking[2] in 2007 revealed that there were almost 80 million microinsurance clients around the globe. By 2013, this figure had increased to over 263 million. Present day, experts believe that these numbers might have yet again doubled. A large part of this growth has come from the spread of mobile insurance products, which are able to reach scale very rapidly. Annual growth rates show that while mature insurance markets grow between approx. 2-4% annually and emerging insurance markets by approx. 10-12%, mobile microinsurance has shown annual growth rates of 100% or more. For example, in Ghana, technical service provider Tigo reached 1 million clients only one year after launch, and in Bangladesh, Grameenphone and MicroEnsure reached 1 million clients within 30 days. The application of digital technology in inclusive insurance has already drastically changed the inclusive insurance landscape and holds much promise for the future.

> ***It takes one year to insure 1m lives via MNOs vs. 40 years for a typical insurance market***
>
> *Accenture*

1 GSMA, 2015. *Mobile Insurance, Savings & Credit Report*. http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/08/Mobile-Insurance-Savings-Credit-Report-2015.pdf

2 Accenture, 2014, Mobile Microinsurance (MMI): goes from experiential to exponential. Presentation by Thomas Meyer at the International Microinsurance Conference (IMC) Mexico.

Figure 1.

Source: Inclusivity Solutions

Characteristics of Mobile Insurance Business Models

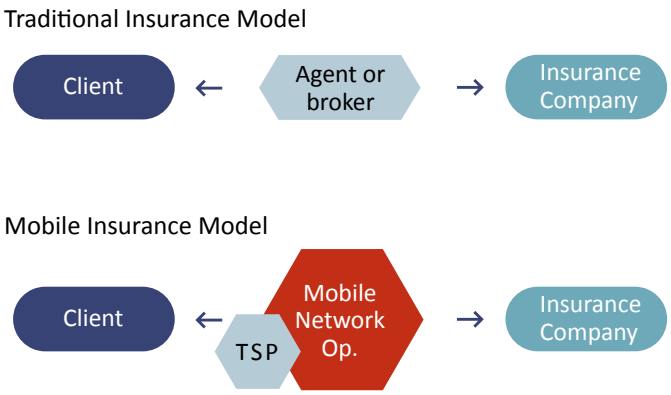
A mobile insurance model refers to an insurance business model that uses the mobile phone channel for any part of the insurance product lifecycle. The number and nature of new entities involved, the digitalisation of the insurance value chain and the application of Big Data analysis are the primary characteristics setting mobile models apart from traditional insurance business.

Emergence of New Players

One of the defining characteristics of mobile insurance models is the introduction of new actors into the insurance value chain. While the structure of traditional insurance models is characterised by a client, insurer and agent or broker intermediary, mobile insurance models introduce multiple new actors into the value chain who typically originate from outside the insurance sphere: mobile network operators (MNOs) or other third party aggregators leverage networks and provide insurance to a largely pre-existing clientele, while technical service providers (TSPs) act as intermediaries between the insurer and the MNO by offering the administrative and payments infrastructure, though they are also often involved in product design. Either of the three stakeholders can take the lead in the provisioning of insurance. However, it is often the MNO who drives the initiative. A recent study found that 63% of mobile insurance services were led by MNOs[3]. When an insurer takes the lead, the MNO plays a largely passive role, supporting transactions via their mobile operator and/or mobile money infrastructure, while the insurer, who is regulated by the insurance supervisor, underwrites the product. In MNO-led models, the insurer is allowed to use MNO data to target and enrol clients. In this model the MNO provides its considerable brand strength to stimulate take-up of insurance as the product is embedded in the package offered by the MNO. MNOs offer insurance to increase customer loyalty, reduce churn, create brand awareness and/or increase average revenue per customer. The MNO's investment may include paying premiums on behalf of their subscribers, leveraging their own infrastructure, using Big Data to target clients and/or co-funding marketing and advertising. The MNO, as the aggregator, holds the customer base, provides a 'trusted brand' and a ready premium collection mechanism. MNOs are not traditionally under the jurisdiction of the insurance supervisor.

3 GSMA, 2015. *Mobile Insurance, Savings & Credit Report.* http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/08/Mobile-Insurance-Savings-Credit-Report-2015.pdf

Figure 2. Traditional Insurance Model | Mobile Insurance Model



These new players and technology-driven partnerships are impacting the insurance value chain and power balances in the market, presenting particular challenges for supervisors. Moreover, the inclusion of new players from the non-insurance sphere may cause a misalignment of incentives between them and insurers, which could condition sales and potentially distort customer perception of insurance, exerting downward pressures on demand.

Digitalisation of the Insurance Value Chain

The pervasiveness of new business models is largely due to the enhanced efficiency and lowered transaction costs allowed by the use of information technologies in each stage of the insurance value chain. Customer acquisition, product design and distribution and customer relationship management are all greatly facilitated by the use of mobile network data. The use of technology in mobile insurance partnerships has the potential to overcome many of the traditional barriers across a number of elements of the inclusive insurance product lifecycle, ultimately enabling scale.

- **Digital data generation, communication and analytics** are used to inform insurers about customer preferences and behavioural patterns. The processing of large volumes of digital information can indicate a potential customer's propensity to take up insurance or estimate their willingness to pay. Digital data analytics and increasing data integration allow companies to improve their prediction capabilities; such analysis can be leveraged to improve customer targeting, marketing, product design, to tailor distribution and to reduce churn.
- **Digital contracting:** mobile phones provide an easy and low-cost channel to communicate with prospective clients and originate policies via electronic signatures.
- To **lower distribution costs**, insurance providers opt to partner with third party aggregators to facilitate product sales and premium collection. Insurance companies 'piggy back' on their partners' client base and digital infrastructure to decrease costs and reach low-income customers outside of traditional distribution touch points.
- **Premium collection** via mobile channels is less costly to the insurer and more convenient for the target market where policyholders are often unbanked. Premiums are often deducted via an MNO's airtime/data or mobile money infrastructure.

- **Claims settlement:** mobile phones can facilitate speedy claims lodging and settlements, for example when pay-outs are facilitated via mobile wallets. Traditional challenges to claims settlements, such as lack of infrastructure or when consumers lack appropriate documentation, are overcome when using third party aggregators as these entities' existing client relationships and payment streams can be leveraged to lodge and settle claims.
- **Risk modelling:** applying sophisticated algorithms to big datasets can help providers better profile and model the risk they are underwriting to be more efficient at product design, risk selection and premium pricing.

Big Data Analysis

Leveraging the mobile infrastructure through Big Data analysis, insurers have more opportunities to pioneer new products to more consumers at faster speeds. Big Data, which refers to the vast amounts of digital information in structured and unstructured data sets, facilitates both the efficiency and efficacy of the insurance process to an unprecedented degree. Big Data is characterised by three 'v's: (i) very large data volume (Tera- and Petabytes); (ii) velocity of accumulation (often high frequency in real time); and (iii) variety (mobile call patterns, blogs, call centre logs, etc.)[4]. The transmission of computerised information assists in the real-time collection of data and enables insurers to establish direct, unmediated customer relationships based on direct access to unfiltered data. This mapping of preferences and behavioural patterns allows insurers to gain a more precise understanding of who their customers are and how their needs change over time so that they can individualise offerings.

The implementation of new technologies and processing analytics in the mobile infrastructure creates an environment of increased interconnection and information-sharing, which, while bearing the potential to bring insurance to millions of uncovered individuals, creates new challenges in terms of privacy, data protection and cybersecurity.

Rising Privacy Concerns

Despite the potential benefits of mobile insurance, the increasing adoption of pervasive and often intrusive information processing has led to rising levels of privacy concerns around the world. A recent survey conducted by KPMG[5] in more than 24 countries indicated that in 2016, 55% of consumers worldwide opted against buying something online due to privacy concerns. In the same survey, 66% of consumers stated that they were not comfortable with apps utilising their personal information. Rising levels of privacy concerns can also be found in many developing countries and emerging markets. A different survey[6] conducted with over 24,000 consumers across 20 countries revealed that the number of consumers who are 'somewhat' or 'much more concerned' with their privacy compared to one year ago has grown significantly. This increase in privacy concerns can lead to trust issues, which, unless appropriately addressed, can pose an impediment to the uptake of mobile insurance services in the future.

4 Watson, H.J. (2014). Tutorial: Big Data Analytics: Concepts, Technologies, and Applications, http://aisel.aisnet.org/cgi/viewcontent.cgi?article=3785&context=cais
5 KPMG (2016). Crossing the line: Staying on the right side of consumer privacy, https://home.kpmg.com/content/dam/kpmg/au/pdf/2016/crossing-the-line.pdf
6 2016 CIGI-Ipsos Global Survey on Internet Security and Trust, https://www.cigionline.org/internet-survey-2016

Data Protection

Data protection typically encompasses political, legal, regulatory, and technical as well as protocol measures in order to protect personal data[7]. Typically, data protection includes individual protection rights (such as the right to access data, to correct it, etc.) and is normally extended only to individuals, not firms. Depending on the situation in the individual country, there are a variety of laws that could be applicable to data protection.

Core data protection rights for individuals typically include provisions such as the transparency of data processing practices; that is, organisations that collect personal data must be open and clear about their processing matters. Personal data needs to be collected for limited and lawful purposes and must not be used for any other purposes than the ones stated at the time of collection. The purpose of the disclosure also needs to be specified. In many regulatory regimes, individuals have the right to consent to the processing of their data, which is insofar fundamental as it increases the transparency of processing. Moreover, data protection laws also direct technical and procedural safety measures in order to prevent unauthorized access to data. Other provisions include that data must be relevant, accurate and up-to-date and that the subject of the data must have the right to access the data and have it corrected if necessary.

Data Protection Challenges in Mobile Insurance

Data Ownership and Responsibility

One of the main challenges arising out of mobile insurance models is the issue of data ownership and data distribution. Who exactly owns client data and who is responsible for its protection and/or dissemination is a complex issue that often depends on the business model and on the servicing agreements between the entities involved. While the mobile network operator (MNO) owns all consumer data that is collected through their mobile network, other entities such as TSPs may be outsourced or take on functions whereby they are given access to customer data from the MNO's database. For example, TSPs may be given data in order to engage in pre-screening to identify customers to whom insurance should be offered. This then allows the TSP to directly engage with the customer to establish a relationship and directly compile additional information about him/her, which is then shared with an insurance provider in order to brokerage a deal. This free-flow of data transfer highlights important consumer privacy and data protection questions as this processing is often done non-transparently without the informed consent of consumers.

Fundamental Shifts Introduced by Mobile Insurance Business Models

Information Asymmetries

Mobile insurance introduces a fundamental shift in the information asymmetries that exist in the market, not only between customers and firms but also between firms and supervisors. Once firms conduct Big Data analyses they process information in a way that is mostly non-transparent for consumers. When a customer applies for insurance they relinquish their privacy in the form of personal information acquired from their mobile data. It is often unclear to consumers, however, the extent to which they give up this immaterial asset; that is, the kind of personal data that is used for estimation and the type of data analysis that is undertaken.

7 According to the new EU General Data Protection Regulation, 'personal data' is defined as: "… any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." Source: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

Since the extent of information processing and analysis is unclear, customers cannot appropriately calculate a trade-off to give their informed consent. The lack of customer awareness raises important consumer protection concerns related to the need to preserve basic consumer rights intrinsically associated with information collection and processing. Moreover, customers are often captured due to power imbalances whereby they do not have alternative means to acquire insurance. That is, to receive insurance, they must sign what is given to them.

Between firms and supervisors, while supervisors are tasked with monitoring firms that use Big Data analysis, these companies often utilise sophisticated models that complicate the ease of oversight. The use of machine learning or self-learning algorithms, for example, increases the knowledge rift between firms and supervisors which makes it very difficult for supervisors to appropriately supervise these companies. Moreover, the question of who is responsible for regulating the different parties involved adds an additional layer of complication. While MNOs are supervised by the telecommunications regulator and insurers by the insurance supervisor, the insurance supervisor must also coordinate with the telecommunications regulator to oversee MNOs and their activities, with TSPs often falling into a grey area. This added dimension of supervisory responsibility further compounds the regulatory obstacles presented by the use of sophisticated technologies.

Market Expansion and Market Saturation

The insurance market typically undergoes two phases following the introduction of these new business models. The first is a market expansion phase followed by a market saturation phase. In the market expansion phase, the fall in transaction costs enable companies to price-in more customers, meaning that more individuals are able to access insurance than before and thus overall consumer welfare increases. However, as competition increases the market becomes increasingly saturated. Companies engage in fierce competition for market shares and thus begin to personalise prices and products based on the information they have gathered on individual customers. The combination of personalised prices and products leads to a fall in consumer welfare as service providers start to price products at consumers' willingness to pay, or maximum level of affordability[8]. Moreover, once a product or service becomes tailored to an individual's preferences, it is difficult for an individual to compare alternative offers as other products are not directly comparable due to differing characteristics. These business incentives change the competitive strategies of firms in ways that can make consumers exposed to predatory practices.

Reversing Access to Insurance? Market Saturation and the Pricing Out of Consumers

Q. Does the move to market saturation mean that low-income individuals will eventually be priced out of the market?

It should be noted that in the market saturation phase the personalisation of pricing does not automatically indicate that low-income clients will be priced out of the market. To maximise profits, service providers would ideally like to set a product's price just below each consumer's willingness to pay threshold. However, this does not always hold in practice. For example, if a firm has customers that have proven to be unprofitable, the firm will set a price that the customers are not willing to pay, thereby pricing them out. It cannot be said that in later stages of market development all low-income individuals will be discriminated against and priced out of the market as some of them might in fact be profitable customers.

8 Ghose, A. and K.W. Huang (2009). Personalized Pricing and Quality Customization, Journal of Economics & Management Strategy 18 (4), 1095-1135. The model presented in the paper is applicable to a saturated market. In an expanding market, net welfare effect for consumers can be positive, if more overall consumer welfare rises from pricing in new customers.

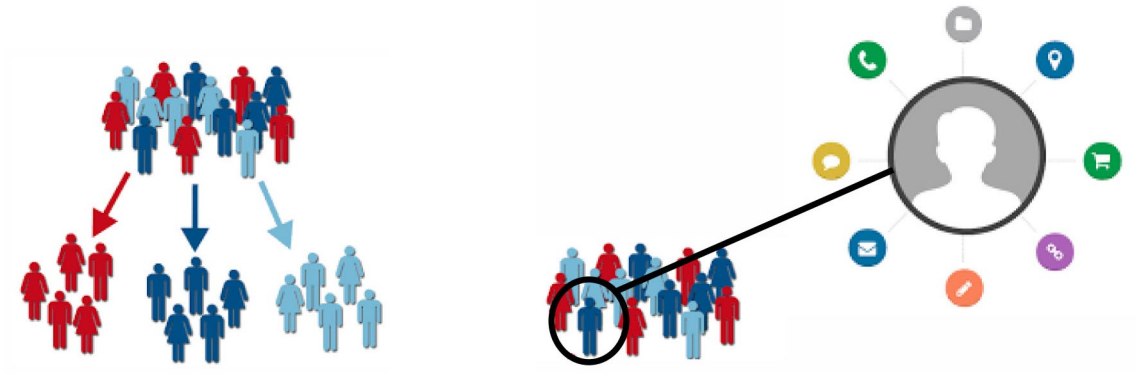
Competitive Strategies of Firms

Mobile insurance business models also lead to changes in the competitive strategies of firms, primarily due to the fact that insurance companies are able to increase the sheer amount of information that they collect and analyse. The use of Big Data processing enables firms to micro-target and pre-select customers that are considered to have a higher propensity to respond to an offer and become paying and profitable customers. Following the profiling and pre-selected sign-up of clients, insurance firms will then try to design products that are tailored to the specific preferences of an individual consumer. The non-standardisation of such products decreases overall product comparability and thus the incentive for firms to apply tailored pricing also arises.

Privacy: Constructing a 360-Degree View of the Consumer

In traditional insurance models, insurers conduct market segmentation according to observable consumer demographics and behaviour, effectively sorting individuals into different kinds of customer classes. With mobile insurance and Big Data processing, however, firms are able to employ personalised targeting due to the sheer volume of information gathered on customers. The geo-location of individuals, the length and volume of calling patterns, and the duration and direction of calls are only a handful of the hundreds of variables used in the modelling of consumer profiles. These variables reveal sensitive targeting information spanning from an individual's social network and income to the status of their health, commuting patterns and even religion. The information gleaned from the implementation of Big Data analytics is then used to construct a 360-degree customer view that was not previously possible under traditional market segmentation.

Figure 3. Customer Segmentation versus Personalisation



Considerations for Supervisors

With the increasing deployment of information technologies for the provision of mobile insurance, more and more market players collect personal financial, geo-locational and lifestyle information on individuals. This unprecedented transfer of information raises important privacy concerns related to the processing and distribution of personal data as well as consumer protection challenges arising from changes in the competitive strategies of firms. There are undoubtedly significant opportunities that mobile insurance provides in terms of increasing financial access and supporting socio-economic development. However, it is important that supervisors address the issues arising from mobile insurance to ensure that regulation facilitates inclusive insurance market development whilst still protecting policyholders and balancing financial stability.

Regulatory Framework

The aforementioned strategies and shifts borne out of these new digital configurations lead to a host of consumer protection concerns. Supervisors can nevertheless take first steps to address these challenges through appropriate regulation.

While some jurisdictions are considering issuing specific mobile insurance regulation, in others, legislation more generally applied to inclusive insurance is also applied to the regulation of mobile insurance and data protection. Regulating mobile insurance and consumer data is often a complex process involving a range of regulatory and supervisory authorities – insurance, central banking, telecommunications and data protection authorities alike. Various regulatory bodies have consumer data protection as part of their mandate. A country's regulatory landscape is thus typically comprised of some or all of the following pieces of relevant legislation: a telecommunications law, an insurance law, a credit reporting law and a data protection law.

→ *Telecommunications Law*

Typically, a telecommunications law does not contain vast clauses or detailed regulations about data protection, though there may be scattered confidentiality clauses requiring firms to keep customers' data and business methods private. This is because the primary objective of the telecommunications law is to regulate the telecommunications market, for example by resolving issues such as the licensing of telecom firms and setting up an authority to regulate the telecommunications system. Data protection measures are not explicitly outlined in telecommunications legislation.

→ *Insurance Law*

The same holds true for the insurance law. The insurance law has the primary goal of supervising the insurance industry in order to develop and maintain fair, safe and stable insurance markets for the benefit and protection of policyholders. As with the telecommunications law, in some countries insurance legislation also contains confidentiality clauses about customer data; however, the insurance law is not fully focused on the preservation of client data privacy.

→ *Data Protection Law*

Regulation explicitly embodying data protection and privacy measures requires the creation of a separate data protection law. Data protection laws typically regulate basic provisions on data collection, processing and analysis, whilst also establishing a data protection authority tasked with protecting the basic rights of data subjects. The structure and scope of data protection legislation can vary greatly, for example between focusing only the private or public sector to covering specific industries within a sector. In many jurisdictions data protection laws are typically overarching bodies of legislature enshrined in the state's constitution, not specifically designed as a subset of insurance regulation dealing with the mobile ecosystem.

→ *Credit Reporting Law*

Some jurisdictions also have a credit reporting law. The implications of a credit reporting law on data protection depend on the scope of the law in each jurisdiction. Some credit reporting laws designate a group of institutions that are able to report to a credit reporting agency; if an insurance company is part of this group of designated institutions then the insurance firm would be able to report its policyholders and payment behaviours to the credit reporting agency. This law might play a role in terms of how information-sharing is operated and monitored in a given country.

→ *Legal Challenges: Status and Compliance of New Players*

The particular structure of a country's legislation can raise many challenges in terms of data protection and data privacy. Non-insurance entities involved in the insurance value chain are primarily outside of the traditional jurisdiction of insurance supervisors (e.g. MNOs are regulated by the telecommunication authority). Yet when these non-insurance entities are involved in the business of insurance, this can pose large consumer protection risks for their vast client base if their actions are not properly supervised. Moreover, in many jurisdictions it is often the case that existing legislation does not take mobile insurance and new players such as TSPs into account. TSPs are often involved in the insurance value chain by supporting different activities but take the lead on managing consumer data; while in some jurisdictions TSPs are required to register as agents under the jurisdiction of the insurance supervisor, in others they fall outside of existing legislation. This regulatory loophole is further compounded if there is no data protection law governing the processing of personal information. It is important that supervisors clarify or adapt the legal framework that TSPs and other intermediaries must comply with in order to protect consumers against issues arising from the Big Data environment.

It is key that there is a harmonised supervisory approach for good practices in overseeing data protection, with any new requirements taking into account existing mandates and regulations. Clarifying who is responsible for protecting what data is critical, as more and more data is being collected by third parties or intermediaries and then used by insurers or other actors for insurance-related business. Supervisors from various authorities should work together to preserve the most fundamental rights of consumers, especially in a Big Data environment characterised by the pervasive and often intrusive collection of personal information. There needs to be a legal basis for this cooperation, ideally codified in a document (e.g. Memorandum of Understanding) that outlines basic procedures for monitoring and regulating the different entities involved.

Data Protection Legislation in Mobile Insurance

Telecommunication law: confidentiality clauses on keeping the customer's data and business matters private

Insurance law: confidentiality clauses on keeping the customer's data and business matters private

Data protection law: data protection provisions regarding collection, processing, analysis and transfer of personal data, tasks for data controllers and right of data subjects (individuals)

Credit reporting law: data protection provisions as well as conditions of transfer of insurance client data to credit reporting agency

Case Studies: South Africa and Mexico

SOUTH AFRICA

Mobile insurance is not a supervisory focus that is explicitly regulated in South Africa. Rather, the cross-cutting issues surrounding mobile insurance, and data protection challenges more specifically, are overseen by a range of supervisory bodies as well as under the common mandate of the South African Constitution.

MNO Insurance Partner Structures and Risks

To understand the different regulatory challenges in the South African context, it is important to understand the structures of the various MNO insurance partnerships and how they operate within the insurance industry[9].

- → **A registered insurer is part of the MNO group:** the MNO has its own insurance company that has been established as part of the MNO group and mostly everything functions internally.
- → **Cell captive arrangements:** the MNO creates a separate entity that becomes a cell owner of the risk insured by acquiring a specific class of ring-fenced shares in a registered insurer. This is often coupled with an outsourcing or binder agreement whereby the MNO performs various functions on behalf of the insurer (i.e. conducts the insurance business) and the insurer underwrites the risk.
- → **Brand arrangements:** a registered insurer takes full responsibility of the insurance, though there are possibly data sharing arrangements with the MNO in order to obtain the customer base. The role of the MNO is to provide data on customer details so that they can aggregate distribution of the product and may receive compensation for the brand arrangements they have with the insurer (as the insurer will be leveraging business off the MNO's brand).

The main risks identified in the South African mobile insurance market are:

- **Data protection and data privacy** issues arise due to the structural interconnectedness of entities and the resultant information asymmetries, which lead to the unauthorised use of data due to the free-flow of information between the different entities. For example, in cell captive arrangements, even though the MNO acts on behalf of the insurer, it uses the information of its parent holding company which could be a breach of data according to South African law.
- Numerous **abusive marketing practices** have been identified, such as negative option marketing[10], lack of identification of the insurer and lack of critical information relating to contract terms.
- **Operational risks** specifically related to the outsourcing of functions and partnership risks: this includes a lack of oversight of the entity conducting the insurance business on behalf of the insurer, which results in inappropriate consumer protection throughout the lifecycle of the product. This is particularly prevalent in cell captive and binder agreement structures.

9 Only the three most common structures are listed. However, a specific MNO's structure is not necessarily limited to one of these structures and could comprise a combination of any of them.
10 An example of negative option marketing is an insurer selling bundled products, such as providing free funeral insurance for a given time period then afterwards automatically deducting premiums without the policyholder asking to continue with the policy.

Regulatory Framework

The current regulatory framework governing mobile insurance and data protection consists of:

- The **South African Constitution:** the overarching legislation that governs all conduct and entrenches the Bill of Rights. All laws in South Africa must be consistent with the Constitution. There is a provision in the Constitution stating that every citizen has the right to privacy. Although it is not a detailed legislation it provides the overlay for other laws referring to data privacy.
- The main Act governing data protection in South Africa is a law that has general application called the **Protection of Personal Information Act (POPI)**. POPI establishes an information regulator (note: not the insurance supervisor) and gives them extensive powers to administer the Act. POPI also deals with data processing and grants certain privacy rights to the connection to and analysis of data from individuals in South Africa. It is thus a general Act that applies to all insurers, as there is currently no legislation in the insurance regulatory framework specifically governing data protection[11].
- Another law that has general application is the **Consumer Protection Act (CPA)**, which has limited privacy provisions. However, the CPA does not apply to a function, act, transaction, goods or services that are subject to financial services legislation[12]. The financial services industry therefore has its own consumer protection laws governing their conduct.
- There is also an **Electronic Communications and Transactions Act** which has some provisions on data protection.

Overall, the main body of legislation governing data protection in South Africa is the POPI Act. The challenge for the insurance regulator is to establish appropriate Memorandums of Understanding (MOUs) with the information regulator in order to cooperate with dealing with insurers when any data protection laws have been breached.

Risk-Mitigating Actions Undertaken by the Financial Services Board (FSB)

Proposed amendments to legislation

Currently, the Long-term Insurance Act and Short-term Insurance Act, which govern insurance in South Africa, do not contain specific requirements on data protection nor mobile insurance. Nevertheless, the FSB is working on subordinate legislation to address issues on data privacy and consumer protection. While these amendments do not have a mobile insurance-specific focus, they are by nature applicable to Big Data analysis and mobile insurance. One important amendment addresses various issues around data management, which will place significant requirements on insurers to have a data management framework for Big Data analysis. This will address concerns around outsourcing arrangements by enforcing the accountability of the insurer and placing strict requirements on oversight, product design and monitoring. Similar requirements relate to other important issues such as disclosure, advertising and negative option marketing. These requirements are media-neutral, meaning that the legislation applies to any platform, mobile or otherwise. All of these policies, albeit general, will have a significant impact on mobile insurance.

11 Although POPI has been enacted, all the substantive sections dealing with data processing and privacy have not yet taken effect. Only sections that are of an administrative nature (for example establishment of the information regulator) have, to date, taken effect. It is unclear when the substantive sections will be made effective but it is anticipated that it will occur in 2017.
12 Section 28(2)(b) of the Financial Services Board Act refers.

While not bringing in robust privacy or data protection laws into insurance regulations, the FSB is in the process of proposing amendments that will indirectly provide the insurance regulator with the ability to take action where data protection infringements have taken place[13]. The FSB will also need to enter into a MOU with the information regulator to incite cooperation and action as deemed necessary.

Targeted supervisory approach

To complement legislation, the FSB is considering adopting a targeted supervisory approach through which to regulate issues of mobile insurance and data protection. This could entail targeting mobile insurance providers and ensuring that they comply with the relevant pre-existing legislation.

MEXICO'S DATA PROTECTION REGIME

Mexico's personal data protection regime is comprised of a constellation of laws codified in the Mexican Constitution. The Constitution states that all information concerning the private lives and personal information of citizens is protected under the terms determined in legislation and is recognised as a guaranteed fundamental right. Compliance is guaranteed by an autonomous federal body, *the National Transparency, Access to Information and Personal Data Protection Institute (INAI)*, which is responsible for protecting the personal data of all Mexican citizens. The insurance supervisory authority, the Mexican Insurance and Sureties Commission, is not mandated with regulating data protection.

The main laws pertaining to the regulation of data protection in Mexico and their provisions are outlined below.

General Transparency and Access to Public Information Law

- Creates the National Transparency, Access to Information and Personal Data Protection Institute (INAI), an independent body charged with supervising the use of personal data
- Access to personal information is allowed only to its rightful owners, representatives or authorised civil servants
- Holders of personal data must protect the data and may allow access to confidential information only with the consent of the information's rightful owner(s)
- Establishes an appeal instance before INAI

Federal Transparency and Public Information Access Law

- Defines INAI's structure and role
- Establishes Transparency Committees within the federal government to uphold transparent data processing

13 This includes a proposed amendment that will require that an insurer must comply with all relevant legislation relating to confidentiality, privacy, security and retention of data or information.

Federal Law for Protecting Personal Data in Possession of Private Individuals

- Regulated subjects include individuals and entities obtaining, utilising, disseminating or storing personal data
- Obliges entities who treat personal data to obtain such information without deceit and to use it with the explicit consent of its owners. Such entities must tell their owners that information is being obtained and with what purposes by means of a Privacy Notice.
- Allows entities in possession of personal data to transfer the data to third parties without the consent of their owner when such transfer is made to subsidiaries of or any other company in control of the responsible entity
- Establishes that the holders of personal data enjoy the rights of access, correction, cancellation and opposition

Financial Groups Regulation Law

- The company in possession of personal data and any other financial entities belonging to a financial group may share information relating to the services undertaken by each entity with their clients without it being an infringement on the secrecy, as long as the nature of the shared document implies the obligation of secrecy

Financial Services Users' Protection and Defence Law

- The National Commission for the Protection and Defence of Financial Services' Users will create and update a Registry of Users who do not wish their information to be used for marketing and advertising purposes
- Financial institutions are forbidden to use the information contained in their clients' databases for marketing or advertising purposes and to send advertisements to those clients who have explicitly said they do not wish to receive it or who have registered themselves in the User's Registry

Insurance and Sureties Institutions Law

- Insurance institutions may share information for purposes of strengthening the measures to prevent and identify operations supporting criminal association without such exchange of information implying the infringement of confidentiality obligations

Questions and Discussion

The average low-income consumer is typically not aware that they have rights to defend. Are there any measures to sensitise people as to where their consumer rights might be violated with regard to data protection issues?

This really depends on the country. In some countries under the data protection law, not the insurance legislation, the companies that collect and process personal data must inform consumers of their activities; consumers then have specific rights to check the accuracy of the data gathered and to have any discrepancies rectified. However, this is not universally prescribed so customers are often unaware of their rights. How consumers typically hear of abuses generally comes from the media.

What can supervisors do if there is no overarching data protection law in their regulatory framework? What can be done with an insurance law?

This very much depends on the scope of the pre-existing insurance law and how empowered a supervisor is to implement consumer protection measures in related provisions. If the possibility exists, it is important that supervisors push the data and privacy responsibility back on to the insurer. Basic data protection rules that could be implemented would be enhancing customer knowledge on data collection, processing and use.

Is lack of complaints on the topic of data protection really an indicator of lack of abuses? Or are abuses very often hidden to the consumer because he/she is not aware of where breaches can happen, e.g. of his/her privacy?

The issue of lack of complaints is associated with the non-transparency of the Big Data environment. The non-comparability and non-standardisation of electronic services puts customers in a position where it is difficult to detect any sort of discrimination. From a regulatory perspective, the lack of complaints is not an ideal indicator. However, in some jurisdictions it may not be a primary focus for insurance regulators, as there may be overarching data protection legislation that puts the responsibility of consumer protection under the purview of another authority. Insurance supervisors must cooperate with other regulators to proactively address these issues, whether through a supervisory approach targeted towards mobile insurance specifically or through a more general application.

What competitive effects should supervisors be wary of in the future?

Complicated vertical competitive effects typically emerge from the configuration of the mobile insurance business model. For example, MNOs are often strategically driven to engage with insurers and TSPs to provide insurance in order to increase their customer loyalty, reduce churn, create brand awareness and/or increase average revenue per customer. In turn, TSPs are incentivised to engage in insurance business as they receive a kickback for the deals they broker as intermediaries. These incentives can lead to power imbalances in the market and give rise to strategies aimed at exploiting the opportunity to create a lucrative business for the parties involved, rather than ensuring that products and prices are appropriate for the end consumer. Supervisors must be wary of perverse market incentives and should look at whether services are bundled and whether consumers have the choice to take up insurance from the particular TSP or insurer. What can happen is that if consumers don't have a choice, they can be involuntarily captured by the market dominance of a particular insurance company.

How can insurance supervisors regulate mobile insurance intermediaries to ensure that they are responsible distribution channels for insurance?

There are a great variety of approaches and requirements supervisors adopt to regulate mobile insurance intermediaries. In some countries, TSPs are registered as brokers or underwriting agents for insurance. Yet in others, the MNO is deemed as the distribution channel and thus must register as an agent, effectively bringing them under the scope of supervision. Ultimately, how an intermediary should be registered and to which regulation they must comply very much depends on the specific functions that they undertake. Outsourcing, in addition to value functions, must also be defined. For example, if an insurer outsources a function to another entity, the insurer must accept liability of the body issuing insurance on its behalf.

How are data ownership responsibilities distributed between the MNO, insurer and TSP and how can these responsibilities be established – for example, through regulation, a Memorandum of Understanding or through other measures?

Typically, an MNO, an insurance company and a TSP would determine these responsibilities in their own contracts with each other. Depending then on the regulatory regime, assuming a general data protection law exists, each of the institutions that collect information are responsible for that information. Once an entity collects data it falls under the data protection law and thus must adhere to the rules set out in the legislation. That said, if an insurance company is outsourcing a critical function like underwriting or administration, then the insurance company is typically responsible for the entity to which they have outsourced this function, including all of the information processing issues that come with it.

Is using the minutes of the mobile service (airtime) to pay premiums considered a form of electronic money (e-money) transfer? Have there been any examples of conflicts with e-money transfer legislation?

This is a difficult question that depends on the country context. While some emerging and developing countries do have e-money laws or regulations, in others airtime is either not considered an electronic payment scheme or the situation is undefined. For example, in South Africa, e-money transfers have not been included in the regulatory framework because it has not presented itself as a prevalent issue in the market. The issue of whether or not airtime can be considered a form of money is still a topic that many Central Banks are discussing.

Are there confidentiality issues involved in the freemium model and can client data be used without client consent?

This depends on the manner in which the model is implemented. If clients don't specifically agree to sharing data then there would be a data protection issue. There needs to be a simple, transparent and easily understandable manner in which clients are informed about what happens to their data and how their data is used. Ways to give consent (or to deny consent) need to be simple and if someone doesn't agree to having their data shared, then this must be respected. In addition to the models that are used, the regulatory framework is also important. In some countries, there is an 'opt out' approach, i.e. data and all information can be shared unless the consumer explicitly states that the data cannot be used. This could pose problems for clients. By contrast, if the regulation requires that data cannot be shared unless the consumer explicitly consents to sharing/using the data, there is more consumer protection.

Access to Insurance Initiative
Hosted by GIZ Sector Project Financial Systems
Approaches to Insurance
Deutsche Gesellschaft für Internationale
Zusammenarbeit (GIZ) GmbH
Dag-Hammarskjöld-Weg 1-5
65760 Eschborn, Germany

Telephone: +49 61 96 79-1362
Fax: +49 61 96 79-80 1362
E-mail: secretariat@a2ii.org
Internet: www.a2ii.org

The Initiative is a partnership between:

Hosted by: