The Impact of IoT on the Home Insurance Industry

Valeria Savatteri

September 6, 2018

Master Thesis

Copenhagen Business School

Master in Management of Innovation and Business Development

Supervisor: Lars Bo Jeppesen

Student Number: 113811

Table of Contents

Abstract 3

Introduction 4

- Aim of this thesis 4
- What is a smart home? 4
- Smart home adoption in Europe and the US 6
- Evolution of home insurance in Europe and the US 8

Literature Review 11

- Adverse selection and moral hazard in the insurance market 11

Theoretical Analysis and Framework 14

- IoT, Risk Assessment and Insurance Service Model 14
- Data Capitalism in the Insurance industry 16
- IoT as a source of new risks and challenges for Home Insurance 19

Empirical Analysis 24

- Hypothesis formulation 24
- The Data 25
- Frequency Analysis 27
- Correlation Analysis 33
- Factor and Regression Analysis 36
- Limitations of this study 41

Results 42

Discussion 45

- Hypothesis verification 45
- Implications for the relationship with insurance companies and their customers 47
- The future of home insurance 49

Conclusion 51

Exhibits 55

- Exhibit 1 – List of insurance companies considered 55
- Exhibit 2 – List of variables analyzed 55
- Exhibit 3 – Table of extracted communalities (United States) 57
- Exhibit 4 – Table of initial eigenvalues and extracted factors (United States) 57
- Exhibit 5 – Regression of Loss Ratio against factors (United States) 58
- Exhibit 6 – Regression of Expense Ratio against factors (United States) 58
- Exhibit 7 – Regression of Combined Ratio against factors (United States) 59

Exhibit 8 – Regression of Market Share against factors (United States) 59
Exhibit 9 – Table of extracted communalities (Europe) 60
Exhibit 10 – Table of initial eigenvalues and extracted factors (Europe) 61
Exhibit 11 – Regression of Loss Ratio against factors (Europe) 61
Exhibit 12 – Regression of Combined Ratio against factors (Europe) 62
Exhibit 13 – List of professionals interviewed (March-April 2018) 62
References 64

Abstract

Connected devices are becoming the new normal, and our homes today are almost a sci-fi dream compared to domestic life 50 years ago. Nevertheless, homeowners' insurance has not changed much in the last decades, except from sporadic ratemaking adjustments and the constant rise of annual premiums. The scope of this thesis is to provide a theoretical and empirical overview of how property insurers are coping with the rise of smart home technology, in terms of changes to their policy structures, risk assessment models, reliance on IoT data and, ultimately, the relationship with their customers. A literature review revealed that data from IoT devices may prove useful in mitigating two structural problems of the insurance industry, namely adverse selection and moral hazard arising from asymmetric information. Data from Smart Home devices provides new credible ways of screening and signaling, makes it able to recognize high-risk customers and careless behaviors, and makes it easier to detect fraudulent claims.

The second part of the analysis is aimed to demonstrate if, and to what extent, IoT-related initiatives may increase an insurer's profitability by lowering its expense and loss ratios. To this aim, all the homeowners' policy contracts of the major 55 American and European insurance companies were read and searched for IoT-related clauses, and the resulting variables were then summarized in factors. Such factors were regressed against 4 main financial indicators in the two reference markets. It emerged that IoT initiatives are associated to a lower expense ratio, but at the same time with a higher loss ratio: hence, there appear to be more claims, but it's less costly to assess such claims. The final part of the thesis is dedicated to assessing how IoT is expected

to change the relationship between insurers and customers, followed by a collection of experts' opinions on the future of home insurance.

Introduction

Aim of this thesis

Until recently, the Internet of Things was perceived as some niche and futuristic phenomenon, with very little awareness of its possible larger-scale implications that could affect even the most traditional industries. At present, a few innovative and forward-looking insurance companies have started to include IoT in their strategic agendas, laying the foundation for new and compelling value propositions.

The aim of this Master Thesis is to assess the **impact of IoT on the home insurance industry**, both in terms of business model disruption, profitability and implications for the interaction between insurers and policyholders.

Insurance providers allow businesses and individuals to transfer risk, by exchanging an unknown future loss for a known and contained premium upfront. Home insurance, often called homeowners' insurance, is a form of property coverage against losses and damages to an individual's house and the assets it contains. It may also provide indemnity against accidents that could happen on the property's premises.

Indeed, the characteristics of home insurance contracts depend heavily on the nature of its underlying complementary good, i.e. **the home**. Apartments and residential houses have undergone major changes in the last 20 years, as digital technologies and the Internet of Things are increasingly becoming part of our everyday lives. Consumer connected devices are forecast to exceed **$5.9 billion** this year (IHS Markit, 2018): thus, it's clear that no company in any industry can any longer ignore the implications of IoT.

What is a smart home?

The smart home market is a subset of the broader **Consumer IoT** phenomenon, alongside with connected vehicles and wearable technologies. Since its first mention

(American Association of House Builders, 1984), the concept of smart home has been declined in different contexts, from energy management to entertainment.

For this thesis, the definition by Frances Aldrich (2003) is considered: "*A Smart Home can be defined as a residence equipped with computing and information technology which anticipates and responds to the needs of the occupants, working to promote their comfort, convenience, security and entertainment through the management of technology within the home and connections to the world beyond*".

In present-day smart homes, household appliances, heating, lighting, security and entertainment systems are capable of **communicating with one another** and with a **central hub**. In addition, these components can be **remotely controlled** from any room in the home and from anywhere in the world, by means of a phone or any device connected to the Internet.

According to a report by IHS Markit (2016), excluding energy and water control devices, in 2015 the bulk of smart home sales came from **safety and security systems**, such as electronic locks, hazard detectors, and intruder alarms. However, their relative importance is expected to decrease over time, as they would leave the stage to consumer electronic devices.

The smart home market is reaching a **chasm** in the technological adoption curve: consumer awareness is rising, approaching the crucial stage between the early adopter phase and the mass market phase. Nevertheless, a common standard has not emerged yet, mainly due to a **lack of compatibility** among devices from different producers. Thus, users are increasingly relying on independent, plug-and-play solutions that can be installed without completely renovating their home.

To overcome this critical phase, manufacturers must both prove the need for their devices and find ways to overcome the interoperability barrier, that makes it confusing for users to set up multiple platforms to control their devices. Indeed, it will be nearly impossible to reach mass adoption if a standard (de-facto or mandatory) does not emerge.

According to Zion Market Research (2016), the global smart home market is likely to grow at a Compound Annual Growth Rate of **14.5% between 2017 and 2022**, and

reach $53.45 billion by 2022. At present, the most promising geographical markets are **Asia**, **North America** and **Europe**.

Indeed, **Asia**'s socio-economic landscape provides a great opportunity for the region to be a global driver of growth in the smart home sector. The management consulting firm A. T. Kearney expects Asia to account for 30% of the global Smart Home sales by 2030, due to region-specific trends. Japan's ageing population, increasing household income in China, high levels of data connectivity in South Korea and Taiwan will provide a fertile ground for these technologies to spread into upper- and middle-class homes. Nevertheless, this research will focus on the American and European markets, as for the time being this phenomenon is not mature enough in the far-east to provide enough data for a comprehensive evaluation.

Smart home adoption in Europe and the US

A recent report by McKinsey shows that the **American smart home market** has witnessed a **31%** year-over-year growth in the number of connected homes, and registered revenues of $15.4 billion in 2017. Indeed, these results are fostered by the presence of a long-standing single market, a homogeneous legislative framework, widespread customer acceptance and a common network of communication-, energy- and security service providers across the country and its different States.

However, despite the fact that the US is now the largest and most advanced smart home market, penetration is forecast to grow at a much lower rate than in Asia. The American consumer technology market has a great number of long-standing industry players and established consumer buying habits, so one would expect disruptive innovations and new entrants, if they can overcome the high entry barriers, to **gain share very slowly**. In addition, the precarious economic conditions of the so-called "Millennial" generation needs to be factored in. As reported by the US Bureau of Labour Statistics for 2018, the majority of citizens aged 19-35 have student debt, and Millennials who graduated in 2017 face the prospect of paying off an average per capita record-setting $37,712 in student loans. Millennial incomes have also fallen dramatically compared with previous generations: the average Millennial's median earnings in 2013 were 43 percent lower than those of Generation Xers in 1995. Such

high debt and **low income** prevent many Millennials from taking steps that are traditional markers of adulthood, such as purchasing homes and starting families. Nevertheless, customer awareness around home-related IoT is on the rise in the US, as advertising in mass media has increased significantly in the past year and major retail chains such as Target and Wal-Mart have recently started to sell home automation products in many of their stores to retrofit existing households.

The smart home concept is expanding on the other side of the Atlantic as well, as **European** consumers explore new energy management, security, and connected entertainment solutions. The European smart home market is still a few years behind the United States: revenues amounted to **$10 billion in 2016**, and they are expected to grow at a **15% annual compound rate** in the coming years (Parks Associates). The major growth driver for the European market is related to energy management, cost savings and security systems. In particular, this is due to **national energy policies** resulting from European directives, that provide monetary and tax incentives for home renovations, encouraging energy efficiency: examples are the UK Smart Meter Rollout, the German *Energiewirtschaftsgesetz*, or the Italian *Strategia Energetica Nazionale* (Balta-Ozkana et al., 2014). Nevertheless, underlying **housing stock characteristics** vary greatly across European countries: physical outline and size of a residential home, strength and coverage of communication signals, and age of the residential buildings are likely to affect the type of interventions that might be implemented. The latter is a critical issue in a country like Italy, with plenty of historic centres to preserve and ancient buildings which are not suitable for most smart-home technologies. In addition, the European population is aging rapidly, and this is expected to increase the demand for home healthcare in the near future.

A report by Statista expects the above-mentioned regional differences in smart-home related revenues to be smoothed out by 2020, with expected revenues of $32.8 billion in the US and $27 billion in Europe, led by smartphone and high-speed internet penetration. However, such **structural differences** between the two markets, each with their own challenges and opportunities, are bound to shape not only the evolution of the home appliance industry, but also every other good and service that is somehow related to European and American homes.

Evolution of home insurance in Europe and the US

One of the most important services related to the home is property insurance. The history of this financial instrument can be traced back to the Great Fire of London, which in 1666 destroyed more than 13,000 houses. After some unsuccessful schemes, in 1681, economist Nicholas Barbon and associates established the first fire insurance company, the "**Insurance Office for Houses**", backed by the Royal Exchange to insure brick and frame homes (Dickson, 2016). The first property insurance company still extant was founded in 1710 as the "*Sun Fire Office*" now, after many mergers and acquisitions, known as the RSA Insurance Group.

In Colonial America, **Benjamin Franklin** made the practice of property insurance against fire common and standard, in the form of perpetual insurance. In 1752, he founded the Philadelphia Contributorship for the Insurance of Houses from Loss by Fire. This insurance company, as the saying goes, refused to cover wooden houses, for which the risk of fire was too great (White, 1998).

In the first half of the 20th century there were **separate policies** for the various perils that could affect a home: a homeowner would have had to purchase separate policies covering fire losses, theft, personal property, and the like. During the 1950s, policy forms were developed allowing the homeowner to purchase all the insurance they needed in one complete policy (Wiening et al., 2002). Homeowners' insurance evolved from simple fire coverage to a **multiple-line policy**, including both property insurance and liability coverage under an indivisible premium (i.e., a single premium paid for all risks).

In the US, standardized policy forms are in place, dividing coverage into several categories. Typically, coverage limits are provided as a percentage of the primary and most comprehensive Coverage A, which is the coverage for the main dwelling (Nance, 2003). Over the centuries, covered damages **extended beyond fire**, and to date they encompass three categories of home-related perils, summarized by the Insurance Service Office (ISO) and the International Risk Management Institute (IRMI) as:

1. **Basic "named" perils**. They are the most basic category, that is, those most likely to result in a total loss, and are mandatory for every insurance coverage. "Named" perils policies imply that coverage is provided only for losses that are

specifically listed on the policy: if it's not listed, it's not covered. Among these perils we can find fire, lightning, windstorm or hail, explosion, smoke, aircraft or vehicle collision, vandalism or riot.

2. **Broad "named" perils**. They expand on the basic form by adding 6 additional perils: burglary-related damage, falling objects, weight of ice and snow, freezing of plumbing, accidental water damage and damages from artificial electricity.
3. **Special-form** (also called all-risk or open-risk). This coverage is the most inclusive option, providing coverage against all fortuitous causes of loss unless specifically excluded. Special-form excluded perils are ordinance of law, earthquake, flood, power failure, neglect, war, nuclear hazard and all intentional acts.

However, the world has changed dramatically since the 1950s, and so have our homes. Dishwashers, televisions, washing machines and other household appliances are no longer luxury items: they can be found in every home and bought at a reasonable price. Many households are now equipped with solar panels and can produce their own electricity. It is now possible to activate an alarm system, turn on the lights, and regulate the heating from anywhere in the world. In all likelihood, our everyday life today is almost like **a sci-fi dream** compared to domestic life in the "good old days". Nevertheless, homeowners' insurance has not changed much since then, except from sporadic ratemaking adjustments and the regular rise of annual premiums, especially in the US.

Indeed, the home insurance industry has reached its mature lifecycle stage and has been under a lot of **pressure** in the recent years. Fierce competition and lack of product differentiation are leading to significant revenue reduction for the majority of players. Considering the broader economic environment, European and American insurers need to cope with growing but still low interest rates, irksome unemployment and low wage- and income growth, that challenge the sector by depressing savings and preventing insurers to rely on their investment income. In addition, geopolitical uncertainties such as Brexit negotiations in Europe and international tensions in the US could impact insurers by negatively affecting economic growth and creating volatility in financial markets (Moody's, 2017). Moreover, tightening government budget coupled with longer life expectancies are driving the demand for health and retirement

products, but at the same time they are increasing insurers' risks and indemnity costs. From a regulatory standpoint, the implementation of the General Data Protection Regulation (GDPR) and Cybersecurity Requirements for Financial Service Companies will require a lot of effort from insurance companies to protect their customers' personal and sensitive data.

In Europe, it is still hard to foresee the economic impacts or the macro societal effect of **Brexit**, let alone the "end state" for the UK's trading relationship with the EU concerning insurance services. Insurers need to continue with Brexit contingency plans on the worst-case assumption that the UK will leave the single market, ending reciprocal passporting of insurance services between the UK and the EU. This would mean that UK insurers currently operating through branches and providing insurance services cross-border in Europe will no longer be able to rely on EU single market rights to underwrite policies and pay claims, and insurers currently passporting in to the UK will no longer be able to underwrite and pay claims in the UK (DLA Piper, 2017).

It is clear from every news headline that the US is witnessing a rising trend on **protectionism**, imposing heavy tariffs on the imports of essential commodities such as steel and aluminum, as a consequence of "national security concerns" (Forbes, 2018). This lays a dangerous precedent: applying arbitrary tariffs and then justifying them towards the WTO on grounds of national security clearly paves the way to tit-for-tat countermeasures from foreign trade partners, eventually leading to a much more hostile international environment. Should these protectionist measures expand to the insurance market, they would block or curtail the expansion of global insurers and, inevitably, have profound impacts on local players.

However, in spite of these challenges and rising uncertainty, a number of forward-looking insurance companies are keeping an eye on the latest trends and are starting to **integrate smart home** and **IoT solutions** within their policies, both in Europe and in America. For example, as early as 2014 BNP Paribas Cardif Italia launched Habit@t, an integrated platform system that controls the house through installed sensors and, in case of danger (fire, smoke, flooding or blackout) sends an alarm to the customer, the operation service and the insurance's assistance center. In the US, American Family is collaborating with NEST to offer 5% premium discount to the owners of NEST

smoke detectors, and further discounts for the purchase of smart doorbells. In addition, the insurer is also committed to reimburse the deductibles of homeowners who suffered a fire or break-in after investing in such devices.

Indeed, these initiatives are symptoms of an increased awareness among insurers about the opportunities offered by connected homes. However, the real challenge will be **integrating the data** provided by smart home devices within existing insurance policies. Such data will undeniably be massive in volume and, most likely, sensitive, requiring insurers to update their existing data storage, security and analytics capability in order to scale up quickly. This will have profound implications on risk measurement, policy design and personalization of insurance products, paving the way for constant and real-time monitoring of anything that happens within their customers' homes.

In the next sections an **overview of the literature** will be presented on the issues of adverse selection and moral hazard in an insurance setting. An **analysis of such theoretical evidence** will follow, to highlight how and to what extent data from IoT devices can diminish the impact of adverse selection and moral hazard on home insurance policies and related claims, how it is expected to increase insurance profitability and what are the challenges IoT will likely bring to industry players. Then the current state of the industry will be examined, by analyzing the occurrence of **IoT-related clauses and initiatives** among the European top 30 and American top 25 property insurance players, in an attempt to discover to what extent such initiatives are related to profitability. Finally, **the results** of the quantitative analysis and the **implications** for the relationship between insurance companies and their customers will be discussed.

Literature Review

Adverse selection and moral hazard in the insurance market

The world of insurance may appear complicated, or even somewhat dull, to the eyes of the layman: in fact, it's sometimes referred to among academics as "*the most misunderstood industry*" (Kunreuther, Pauly, & McMorrow, 2013). The general consumer tends to **view insurance as an investment**, rather than a protective activity: if they haven't collected on their policy they feel that, in some sense, it was not a good deal – while, arguably, the best return on a policy is no return at all. In addition, it is not

immediately clear that insurance is **most valuable on very low-probability events**: if a given event has catastrophic outcomes, but is very unlikely, it's easy for consumers to think: "*This will never happen to me".*

One of the main challenges for insurers is measuring risk. The probability of such loss events cannot be measured directly, being very small and often dependent on many, often unobservable factors. According to the "market of lemons" theory of classical economics, the pricing of insurance products is carried out in **an incomplete market** (Akerlof, 1970). In fact, the insurer (the seller) has little or no information on the prospective buyer and the probability unfortunate events may occur to her, and there is no financial market for this type of security to rely upon. By its very definition, risk of peril-related damages cannot be measured upfront, as it depends on to the future value of a random variable that cannot be observed at the moment (Denuit et al., 2006). Therefore, insurers must rely on observable proxies (age of the building, neighbourhood, age, education and occupation of the inhabitants, etc.) to measure the probability of an unfortunate event to occur.

As highlighted in the previous section, insurance contracts are highly standardized, and have thus proven to be an excellent testing ground for contract theory. From the academic literature, many studies have found **evidence for asymmetric information** in the insurance industry, with two main consequences: adverse selection and moral hazard (Arnott, 1988).

Adverse selection is defined as "*the tendency of high risks to be more likely to buy insurance or to buy larger amounts than low risks*" (Cummins, Smith, Vance, & Derhei, 1983) and it relies on the fact that insurers are unable to identify high-risk customers ex-ante. High-risk agents are more likely to have an accident, and thus are likely to choose contracts with more complete coverage. **Moral hazard**, on the other hand, is essentially risk taking (Cardon & Hendel, 1998): after an insurance contract has been signed, the behaviour of policyholders may change in a way that makes the risk event more likely to happen. These general notions lead to a well-known property. Under both moral hazard and "relevant" adverse selection, one should observe a **positive correlation** (conditional on observable customer characteristics) **between risk and coverage**. In other words, the frequency of accidents among the subscribers of a

contract should increase with the coverage it offers (Chiappori, Salanié, Salanié, & Jullien, 2004): more comprehensive coverage should be associated with higher realized risk, leading to a loss of profits for the insurer, and could result in increased premiums for all policyholders if not managed effectively.

Akerlof's "The Market for Lemons", the **classical model for adverse selection**, presents two main solutions to the problem: screening and signalling. **Screening** makes it possible for the under-informed party (the insurer) to collect additional information over the risk type of prospective buyers, either through observable characteristics or self-selection mechanisms. Insurers already have some screening mechanisms in place, but are only based on characteristics that can be directly observed: age of the building, location, age and education of the inhabitants, credit scoring, and so forth. **Signalling**, on the other hand, refers to the possibility for the most informed party (i.e. the prospective buyer), to signal their risk level by transferring reliable information to the other party, thereby resolving the asymmetry. The introduction of IoT technology enables homeowners to provide the insurer with data about the current condition of the home, its plumbing and wiring, and with the possibility to monitor the frequency of maintenance in real time: this **enhances the effectiveness of screening**, and provides a **new, credible way of signalling**. Therefore, there are sufficient grounds to believe that the Internet of Things has the potential to reduce the impact of adverse selection on both the insurer's income and customers' premiums.

Moral hazard raises a different issue, being the result of hidden actions rather than of hidden information. After the contract has been signed, the insured party is no longer bearing the full costs of her behaviour, which can change in two ways (Baker, 1996). Before the loss event, the insured may behave less carefully, resulting in more negative consequences that the insurer must pay for (***ex-ante*** *moral hazard*). After the event, insured parties may ask their insurer to pay for more of the damages than what would be required (***ex-post*** *moral hazard*). These claims are often supported by voluntary fact misrepresentation, such as inflating the value of stolen property, lying about the cause of the accident, or extending insurance coverage to other unrelated damages. Customers do not necessarily do it in bad faith: they've been paying insurance premiums for many years, and tend to believe it's a "socially acceptable" way to recoup some of the money they've laid out for insurance (Cohn, 2017). As it will be examined

in the next section, insurers need to account for loss adjustment expenses and settlement delays to verify the correctness of each claim: if there are grounds to suspect insurance fraud, these expenses are likely to increase, leading to a surge in insurance premiums for all the customers.

The stream of data provided by a Smart Home system conveys a real-time snapshot of what is going on in the home, and enables continuous monitoring of risk events. This technology would enable the insurer to **recognize careless behaviours *ex-ante*** (notifying the customer about a possible increase in premium if such behaviour persists), and permit timely **detection of deceitful claims *ex-post***. This would expectedly lead to a decrease in insurance frauds, even minor ones, as it would be easier to discover untruthful claims. Therefore, introducing dynamic policies based on continuously updating risk assessment would reduce the existing inefficiencies in premiums allocation due to adverse selection and moral hazard.

Theoretical Analysis and Framework

IoT, Risk Assessment and Insurance Service Model

In the traditional setting, the calculation of loss propensity and risk exposure relies on the law of large numbers and the spread of associated risk, which, for the sake of simplicity, is treated as **homogeneous**. Individual risk is decomposed on a multi-peril basis, and each peril is associated with a given "score" depending on observable characteristics of the dwelling and its inhabitants, drawn from historical data. Current multi-peril rating practice is based on evaluating each peril in isolation from the others, thus implying that perils are unrelated to one another. (Frees, Meyers, & Cummings, 2011). However, it seems fairly likely that perils may depend on each other, or co-depend on latent variables. Event classification can be ambiguous (e.g., fires triggered by lightning) and unobserved latent characteristics of policyholders (e.g., cautious homeowners who are sensitive to potential losses due to theft or vandalism) may induce statistical dependencies among perils.

Traditional risk assessment is therefore defined *a-priori*, that is, based on historical data gathered before the signing of a policy contract. In reality, such risk exposure does change over time, even for relatively "static" assets like real estate.

These changes are associated with both global and local phenomena. Climate change, for example, can shift the spatial distribution and intensity of weather related loss events (Mills, 2005), while variability of neighbourhood crime may alter the risk of theft-vandalism. Even microscale phenomena such as changes in appliance usage rate or frequency and accuracy of maintenance can have a substantial effect on the actual level of risk and the amount of potential damages. While wider-scale phenomena are usually well documented, and any change of risk levels arising from them can be accurately assessed, small-scale phenomena often go unnoticed. The diffusion of smart home systems, however, may dramatically change this condition.

From a technical perspective, an IoT ecosystem is a **Transaction Processing System**: it continuously records and archives all the data of interest and lies the foundation of measuring phenomena. IoT makes it possible to collect real-time data from sensors on the insured property, which can be used for rating parameters and to create **dynamic, continuously updated customer risk profiles**. This constant inflow of data from a variety of sources is bound to change the very definition of risk in an insurance setting, moving from historical data for a pool of “homogeneous” risk to a personalized, risk-based pricing model. The motor insurance was the precursor of this approach, with home and health as the next frontiers.

These continuously updating risk profiles will enable insurers to revise premiums based on how loss- and risk-conditions of the customer change during the policy period, shifting to a “dynamic” and continuously updating risk assessment for a specific customer. Moreover, smart sensors enable fires or water leakages to be timely detected and rapidly confined, thus reducing the entity of the damage and the overall risk, resulting in less burdensome premiums.

This is bound to transform the current offer into more customizable, customer-centric and tailored products. As highlighted above, a first evidence of this trend can be observed in the motor insurance sector: **Pay-As-You-Drive** (PAYD) and **Pay-How-You-Drive** (PHYD) policies are emerging as a consequence of on-board diagnostics and telematics devices installed on newly-built vehicles (Husnjak et al., 2015). Linking insurance premiums more closely to actual individual vehicle - or fleet - performance allows insurers to more accurately price premiums. Clearly, people who drive 35,000

km per year at a high speed are more likely to be involved in a car accident, compared to people who only drive 10,000 km per year at a lower speed. Thanks to usage-based insurance, it is possible to detect virtuous driving habits and charge cheaper premiums to low-risk drivers. This kind of policies also gives policyholders the ability to control their premium costs, as it provides an incentive to use the car less frequently, drive within the speed limit and adopt safer driving habits. Fewer miles and safer driving also aid in reducing accidents, congestion, and vehicle emissions.

Following the example of usage-based motor insurance in a home insurance setting, it's quite straightforward to foresee predictive maintenance services and reduced premiums for responsible behaviours.

Data Capitalism in the Insurance industry

Not only is the world generating more information, but such created information is growing faster than ever before. We can now perform new kinds of analysis that weren't possible when only smaller scales of data were available. Nowadays, big data have an enormous scientific and societal importance and can, ultimately, become a source of economic value because of the predictions that can be drawn from them.

In her paper on Business & Society (2017), Sarah Myers-West defined **Data Capitalism** as "*a system that enables a redistribution of power by means of the commoditization of consumer data, shifting towards the actors who have the capability to access them and extract valuable information*". Such a concept is becoming increasingly widespread in modern society, and emphasizes the urge for nearly every company in the information age to consider data as a valuable asset, and integrate it in their business model.

According to Bankston and Soltani (2014), the falling cost of hardware and processing power is a strong incentive to use big data analytics in a large number of fields. Nowadays, collecting and analysing data is not as labour- and capital-intensive as it used to be. However, in the case of insurers, integrating sensor data into homeowners' policies raises two main issues.

First, insurance providers need to accumulate **sufficiently large amounts** of sensor data before being able to derive useful insights. Following the example above, most Pay-As-You-Drive systems for assessing drivers' behaviour lack sufficient geographic coverage and have few statistical links to data on actual claims. In other words, the sample collected by in-vehicle sensors is limited in size and not yet representative of the whole population of drivers. Until enough data is collected, the insights that can be drawn from these systems will be of limited value.

Second, while it's easier nowadays to pull together large amounts of data, it's important to assess what are the **specific types of data** required to better design policies and enhance the overall customer experience. It's not necessarily true that every type of data IoT sensors can collect will be of some use in assessing customers' risk, or, conversely, data which have no immediate use today may be crucial for future analyses. Indeed, insurers should assess what data sources to hold on to and treat them as a valuable asset: if used correctly, they will provide precious insights to keep their core business profitable.

Speaking of profitability, insurance providers' revenues may come in the form of **policies underwriting** (the main business) or **investment income** from capital gains, dividends and investment activities related to the purchase or sale of security. To the scope of our analysis, only revenues from underwriting activities will be considered, expressed in the form of gross written premiums.

Insurance companies measure their underwriting profitability through the so-called **Combined Ratio**, defined as:

$$Combined\ Ratio = \frac{Incurred\ losses + Loss\ Adjustment\ Expenses + Commissions}{Earned\ Premiums}$$

$$Combined\ Ratio = \frac{Incurred\ losses}{Earned\ Premiums} + \frac{Loss\ Adjustment\ Expenses + Commissions}{Earned\ Premiums}$$

$$Combined\ Ratio = Loss\ Ratio + Expense\ Ratio$$

At its core, the Combined Ratio (COR) is the sum of an insurer's total underwriting costs (net claims, commissions and expenses) divided by total revenues, i.e. earned premiums. It excludes instalments, other operating income and investment returns. It is the sum of two parts: **Loss Ratio** (damages paid, i.e. actual losses over earned

premiums) and **Expense Ratio** (claim verification expenses and commissions over earned premiums). The aim for insurers is to keep the Combined Ratio **slightly below 1**, to maintain underwritings profitable (a combined ratio of 1 is exactly the break-even point), but at the same time to ensure policies are reasonably priced and fit the budget of the customers. To reach this goal, companies must be able to predict losses and loss adjustment expenses (the variable cost associated with investigating and settling each claim) as accurately as possible, and keep premiums slightly above the forecasted expenses.

Data from IoT devices can help home insurance companies to accurately **foresee losses and claim-related expenses** at the level of the single household, based on user characteristics and behaviours that are now observable. Information that may be factored in for calculating premiums is: frequency use of domestic appliances (intensive or sporadic), timely maintenance, peak hours and, in general, users' daily routines. The more accurately outflows can be forecast, the more precisely insurers can price policies and determine risk exposure, and customers will get fairer, more reasonable premiums.

In addition, real-time information can make claim assessments faster and more efficient, while data analytics techniques can **detect frauds** more easily and successfully. If the insurance company is not able to verify the consistency of the information contained in the claims, customers may have an incentive to inflate the amount of the claim to avoid deductibles, misrepresent the facts, or lie about the cause of the accident. This is not a trivial issue, as industry estimates set fraud at about 10% of property and casualty insurance expenses in the US (Insurance Information Institute, 2018). Such fraudulent claims negatively affect other customers, too: in the UK, the Association of British Insurers estimates that fraud adds, on average, an extra £50 (€58) a year to the annual insurance bill for every policyholder.

Thanks to data from IoT devices, it would be much easier for insurers to detect, for example, whether a burglary was staged, or to spot unintentional fires from arsons (some policyholders went as far as setting fire to their own homes). It would be sufficient to check the log of alarm systems in order to detect a break-in. In the future, it may even be possible to inspect the data from smoke detectors to identify the

presence of fire accelerants. This will **lower loss adjustment expenses**, reducing the need for insurers to set aside funds to cover for such overheads – which could be allocated to more productive investments. On the other hand, encouraging less risky behaviours such as better roof maintenance and less overloading of the wiring will lower the frequency, and even the amount, of preventable losses (McKinsey, 2017). These two effects combined will result in **higher profitability** and **lower overall premium**, easing the burden on homeowners and making the policies more affordable.

The aim of the quantitative analysis included in this Master Thesis is to demonstrate that, **by including IoT-related clauses within their policies** or launch similar initiatives, **insurance providers can increase their profitability**, resulting in lower loss ratios and, consequently, lower combined ratios. To date, we are still far from completely dynamic policies: most players go as far as providing premium discounts for the owners of IoT devices, or offering their own connected home platform for a fixed price. However, it's quite straightforward to foresee the industry is heading in such a direction, once more data is gathered and virtuous behaviours can be detected with less uncertainty. To reach this goal, however, industry players need to first tackle a number of technical, legal and customer-related issues which will be presented in the next section.

IoT as a source of new risks and challenges for Home Insurance

After having explored how home insurance companies can create value out of IoT sensor data, it's important to highlight the threats that this paradigm shift can pose to insurers' internal operations, their customers and other key stakeholders. In the following paragraphs, five of the most pressing concerns will be examined.

Smart Home devices collect large amounts of data in real-time, and considering that market penetration of such devices is expected to grow at least by 10% every year (Parks Associates), it is easy to foresee that insurers' databases will be **flooded with several hundred of terabytes** of data every day. As a quick comparison, connected cars generate around 25 GB of data per hour of activity (Hitachi Data Systems, 2016), and it seems reasonable to estimate a connected home might produce a comparable amount, or slightly less.

The first problem to tackle, therefore, is how (and where) to store such data. Prevailing research has shown that the most relevant variables in choosing a Big Data storage tool include the existing environment, current storage platform, growth expectations, size and type of files, database and application mix (Robb, 2016). Within the home insurance context, the area of **cloud computing** has been the most explored. Cloud computing offers groups of servers, storages and various networking resources that can be exploited by Big Data analytics. Therefore, it appears as an efficient way to increase productivity while reducing the cost to process huge amount of data (Almeida, 2017). Nevertheless, it is important that existing enterprise architectures evolve and are able to handle huge amount of data in a fast and reliable way.

Secondly, **data management and analytics** may represent the utmost challenge insurers need to face when entering the realm of Big Data by incorporating IoT in their existing policies. As highlighted by Boyd and Crawford (2015), Big Data does not speak for itself, as often times the relevant information is completely lost in the sheer volume of data. These datasets simply cannot be analysed using the same tools that are suitable for smaller ones, which are often gathered ad-hoc for the purpose. Moreover, a larger amount of data is no guarantee of objectivity: interpretation is at the centre of data analysis and, regardless of the size of the dataset, is subject to limitations and bias. One of the most straightforward biases that can arise in our context is a **sampling issue**. At present, the people who own a smart home system (or have a number of stand-alone devices installed) are usually part of a specific subset of the population: usually young individuals, highly educated, and from the upper middle class. If this bias is not accounted for, in the coming future the mathematical model arising from this data will lower the risk premium only for those customers who use the home in the same way as young, upper-middle class people would (even if a different use would not increase the actual level of risk). Thus, Big Data should not be analysed out of context, and insurers need to draw a clear line on what kind of data should be considered sensitive information that should not be included in the analysis.

This adds to the issue of carefully considering **consumers' perception of privacy and safety** when offering them IoT-related insurance policies. Historically, insurance companies have long been associated with the concepts of protection and customer care. However, the fact that insurers may know what is happening in their clients'

homes in real time (through raw data, but even audio and video files from security systems) is likely to foster feelings of uneasiness and scepticism. The definition of privacy and what can be considered “sensitive information” is becoming increasingly blurred in today’s digital society. Surveys, experiments and anecdotal evidence highlight an apparent dichotomy between self-reported privacy attitudes and actual consumer behavior. This phenomenon is referred to as “***privacy paradox***” (Acquisti B. L., 2015): despite being concerned about their privacy, consumers are quick to give away personal data such as name, email, date of birth, phone number and the like to take advantage of an increased level of service or to obtain a service for free. Despite the argument brought forth by some scholars that decisions about privacy are made under biased risk assessment (Acquisti, 2005), or under the pressure of immediate gratification (Deuker, 2010), according to Flyverbom (2014) it ultimately comes down to the extent to which users trust the platform to be a reliable space for data sharing. This is especially pressing in the case of internet-based infrastructures, but a lack of trust may undermine the willingness to rely on any digital platform.

On the other hand, Varian (2014) points out that consumers already share highly sensitive data with doctors, lawyers and accountants: they do so because they receive tangible benefits in return, and trust these service providers to act in their interest. Hence, insurers need first to measure customers’ willingness to share data from sensors, video cameras, motion cameras and the like – that is, the extent to which consumers trust their insurers’ platforms and data protection capabilities. In accordance with Varian’s view, Accenture’s research shows that most customers would be willing to share personal information with their insurer in return for **tangible benefits**, such as lower premiums or quicker claims settlement (Accenture, 2015). In particular, consumers were more inclined to share information about energy consumption (59%), smoke or carbon monoxide detection (55%), and light sensor information (33 to 38%). According to the survey, they were willing to share security video camera and motion sensor data only if it resulted in faster settlements and greater transparency.

The fourth issue insurers need to consider is to determine whether current safeguards are sufficient to protect consumers’ privacy. The connectivity of an IoT architecture is internet-based, and makes the whole system prone to **cyber-attacks**. A report by Ernst

and Young highlights that a startling 70% of the most used IoT devices contain vulnerabilities, often overlooked by hardware producers (EY, 2015): simply put, more connected devices mean more attack vectors available.

From 2005 to 2017, there have been more than 70 data breaches reported by banks, credit and financial institutions, recently including insurance companies Axa and AMP; for most of these, the number of total records affected is still unknown (ITRC, 2017). In addition, these figures are relative only to the breaches that have been formally and publicly disclosed. As confirmed by Flyverbom's research, data leaks intensify the erosion of trust in internet companies and digital infrastructures, and many breaches fly under the radar as many businesses try to avoid the financial impact, legal liabilities and loss of goodwill that come with disclosure.

Hackers are increasingly **targeting insurance companies** to steal customer information they can use for insurance fraud, and it's easy to foresee that with the advent of IoT sensor data the situation will worsen. According to a research by the New York State Department of Financial Services, most institutions are continuously challenged by the increasing sophistication of cyber security threats and the speed of technological change (NYDFS, 2015). Moreover, many small- and middle-sized insurance companies are vulnerable to attacks because their software is not up to date, or their employees are not trained to spot phishing emails. Even if a company may never be able to foresee whether it will be victim of a cyber-attack (as failed attempts often cannot be detected), researches have come up with a number of guidelines to **minimize exposure**. For example, companies should implement statistical methods for anomaly detection, under the assumption that a cyber-attack will always be reflected in some deviation from the normal patterns, or put in place Artificial Immune Systems (AIS), emphasizing real time and short-term responses (Raiyn, 2014).

Finally, in addition to addressing consumers' privacy concerns and protecting themselves from data breaches, insurers also need to comply with **tightening privacy and security regulation** in Europe and the US, especially on the protection of personal and sensitive data.

From May 25th onwards, the European General Data Protection Regulation (**GDPR**) will enter into force, replacing the current European Data Protection Directive which

was implemented inconsistently within European countries. Among other obligations, the Regulation requires companies to provide consumers with notice and request explicit consent prior to data collection, bearing in mind that the data subject can revoke such consent at any time, with immediate effects. Therefore, policyholders subscribing for a smart-home policy could opt out data collection at any time, without having to wait until renewal. In addition, insurers will be compelled to redesign their systems to provide customers access to their data, and implement security measures such as data encryption and anonymization. Finally, companies will be forced to delete data concerning a particular subject if the data no longer serves the purpose for which it was collected, or if there are no legitimate grounds for further processing. This would mean that insurers will be obliged to delete any reference to previous customers and the data concerning them, upon termination of the policy or earlier, if expressly requested (European Parliament and Council, 2016). Every company storing data of European data subjects must comply with the Regulation by May 26th, 2018, and failure to do so can lead to fines up to €20 million or 4% of revenues.

In the US, the **Cybersecurity Regulation** from the New York Department of Financial Services (NYDFS) entered into force on August 28th, 2017, and concerns all financial services institutions, including insurance providers. In addition to implementing industry's best practices, it requires each covered institution to adopt a robust cybersecurity policy, encompassing data encryption, completion of yearly certifications, enhanced multi-factor authentication and reporting all cybersecurity events, including unsuccessful breaches (NYDFS, 2017). The NYDFS Regulation is a lot more permissive than its European counterpart: it does not specify what are the steps needed to implement its requirements, and does not grant data subjects any additional rights. Nevertheless, compulsory disclosure of all cybersecurity breaches, even minor ones and failed attempts, could undermine the reputation and trust conferred to a number of insurance providers. Highly risk averse consumers may be unwilling to subscribe for a connected home insurance policy, if they knew that a company has been a target for hackers in the past.

Despite GDPR and Cybersecurity Regulation safeguard consumers' interests by imposing higher data security requirements, it must be noted that compliance alone

does not guarantee a company is secure. These days, there is no way to ensure a system can't be broken into, breached or somehow compromised.

In the following chapter, the impact IoT-related claims may have on insurance companies' profitability will be quantified, based on a sample of 55 insurance providers active in the European and American markets.

Empirical Analysis

Hypothesis formulation

In the second part of this Master Thesis, will perform a **correlation-, regression and factor analysis** will be performed to verify the following hypothesis: in Europe and in the United States, home insurance companies implementing IoT-related initiatives have higher earnings efficiency, hence a **lower combined ratio**. Such initiatives will either be in the form of premium discounts for owners of smart home devices (common in the US), significant discounts on such devices, or selling an end-to-end platform solution for the connected home (only in Europe).

From the previous sections, it emerged that IoT can reduce the probability of loss events ex-ante, but makes it much easier to verify claims ex-post. Hence, one should expect **a more consistent decrease in the expense ratio** (monitoring- and claim verification expenses over total premiums earned) with respect to the other indicators. The hypotheses that will guide the analysis are listed below:

H1. *– Companies implementing smart home insurance initiatives present, on average, a lower expense ratio.*

H2. *– Companies implementing smart home insurance initiatives present, on average, a lower loss ratio.*

H3. *– Companies implementing smart home insurance initiatives present, on average, a lower combined ratio.*

These hypotheses are not mutually exclusive: on the contrary if, for example, the first and the second hypotheses were verified, the third one should follow.

The Data

When approaching the data collection phase, it has been decided to concentrate on the largest home insurance companies in the two markets from a revenue standpoint, not to base the analysis on minor or local players, with the aim to improve data availability and reliability.

For the American market, I started from the 2016 ranking of the top 25 P&C US insurers for 2016 by the **U.S. National Association of Insurance Commissioners,** based on countrywide premium (NAIC, 2016). For the European market, I based my analysis on the 2016 European Property & Casualty ranking by **Fundaciòn Mapfre**, a Spanish insurance group which publishes a number of freely available reports (Fundaciòn Mapfre, 2016). The full list of the analysed companies is available on Exhibit 1.

During the months of February and March 2018, I gathered various **financial indicators** for each company from their 2016 annual reports. I decided to focus on 2016 financial statements, as some insurers had not published their 2017 annual reports at the time the data was collected. The financial indicators gathered are the following: gross written premiums and gross premiums earned attributable to homeowners' insurance lines, combined ratio, loss ratio, expense ratio and market share. For each company I included the founding year and, for European companies, in which country the company is headquartered in. The complete list of insurance companies considered can be found in Exhibit 1.

Starting from this list, during the months of February and March 2018 I read the policy contracts for all their homeowners' insurance options, and contacted the Customer Service if the policy contracts were not available online. The contracts were read in the original version if they were in English, Italian, French or German; otherwise, an online translation service was employed. The goal of this phase was to identify the IoT-related clauses and initiatives currently in place, and recorded them in an Excel spreadsheet according to the following categories:

- **Premium discounts** for owners of specific smart home systems or devices (in general, or brand specific). Example: "*a 10% premium discount is available for customers having a smoke detector installed*". In addition, the maximum discount (in percentage) obtainable through the given initiative was recorded.

- **Discounts** for purchase and / or installation of specific smart home devices or systems, usually in partnership with a specific appliance manufacturer. Example: "*ADT Home Security Program for USAA members: 10% off on installation before taxes and 10% off monthly monitoring charges for ADT Home Security devices*" (USAA, 2018). Together with the initiative, the maximum discount available not combined with other promotions was noted in monetary terms.
- **Allowance**: after a burglary, the insurer offers to reimburse up to a specified sum for the customer to purchase and install a state-of-the-art home security system. This clause is more common in Europe, especially in the UK and Ireland. Allowances were recorded alongside with the maximum amount covered.
- **Platform**: some European insurance companies have started to offer their version of a connected home system, usually consisting of a central hub and a few sensors (sometimes even cameras). Such sensors are placed inside and outside the home and are meant to detect different perils: the most common are smoke detectors, water leakage sensors and devices to send alerts in case of break-in. In addition, the annual fee to be paid by the customer for the platform was recorded in the database.
- **Pilot projects** are IoT-related initiatives implemented by an insurer within a limited time span and among a subset of their customers. It's very common for IoT-related insurance clauses to be rolled out within a pre-defined subset of customers (or in a pre-specified area or State). If successful, pilot projects are rolled out as permanent initiatives, offered to the whole customer base. As a general rule, initiatives were considered to be permanent, unless otherwise specified.

It has to be noted, however, that these categories are not mutually exclusive. As a matter of fact, some initiatives can simultaneously belong to two or more categories: for example, in insurance provider can provide owners of a given IoT device with a premium discount, while simultaneously offering its customers a 20% discount on the purchase of the same device. In addition, such initiative may be implemented as a pilot project within a specified subset of customers. This information was further classified

at a more granular level, according to the scope of the devices concerned. This data was recorded in the following variables:

- **Init_Safety**: initiatives concerning internal or external safety cameras, infrared cameras, motion sensors, and all kind of alarm systems to prevent burglaries and break-ins.
- **Init_Control**: initiatives encompassing home automation devices, such as remotely-controllable windows, lights, HVAC.
- **Init_Fire**: initiatives encouraging the use of connected smoke- and carbon monoxide detectors, fire alarms and sprinkler systems.
- **Init_Water**: initiatives related to water leak detectors, flood sensors, and freeze detectors for the pipes.
- **Init_Energy**: initiatives concerning all those devices meant to reduce a household's energy spending, such as smart thermostats and connected solar panels.

Again, these categories are not mutually exclusive: an insurance provider may launch initiatives concerning a wide range of IoT sensors, even from different producers, providing protection against different perils. To solve for this issue another variable, **Total_coverage**, was added to the dataset. It measures the number of peril categories covered by an initiative according to the aforementioned classification, and ranges from 0 (no category covered) to 5 (covers all the categories).

The complete list of variables can be found in Exhibit 2.

Frequency Analysis

The data presented above has undergone a preliminary frequency analysis in Microsoft Excel, in order to better understand the structure of the two markets and provide the foundation for further investigation.

In the **United States**, the 25 companies analyzed represent 60% of the home insurance market. Among these, 16 have IoT-related initiatives in place, for a total of 25 initiatives (some of them have more than one initiative). These are mainly divided in three categories: premium discounts, discounts for the purchase of smart home

devices, and pilot projects. The latter were treated separately because they are limited in reach and time, and usually are innovative endeavours that need to be tested beforehand. The frequencies are reported below (Figure 1).

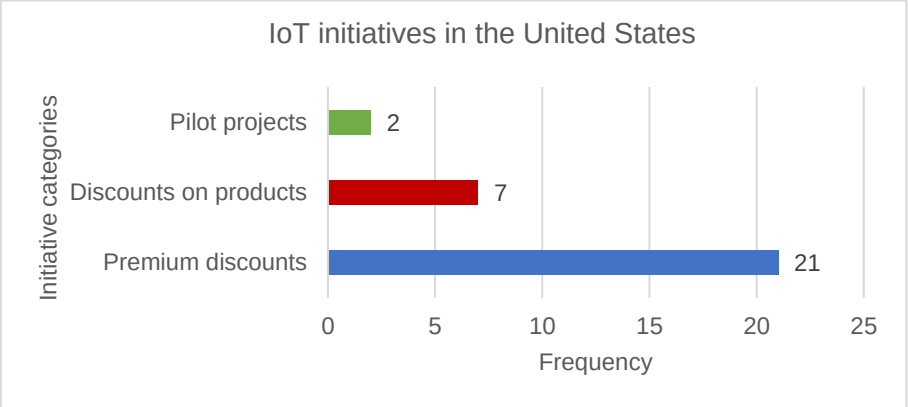

Figure 1 - Different categories of IoT initiatives in the United States

Concerning **premium discounts**, it emerged that most companies have a default clause, granting a 10% premium discount for connected safety- and fire prevention devices ("*Protective Device Clause*"). Some insurers adopted the basic version of the clause, others made some amendments concerning the magnitude of the discount or the category of devices concerned. It is also common for American insurers to offer discounts connected to a specific brand or producer. The most prominent example comes from Allstate Insurance Group, the fourth-largest in the US, offering a 25% premium discount for customers who sign up for a two-year Smart Home Monitoring Plan with Rogers (Allstate, 2018), with a complimentary water leak sensor. A total of 21 premium discounts emerged across the sample, granting an average of 11.06% reduction on annual premiums. As represented in Figure 2, discounts are mostly applied for safety and fire prevention devices, and sometimes in combination with other peril categories.

Figure 2 - Peril categories for premium discounts in the United States

Concerning **discounts for the purchase of smart home devices**, they are usually tied to a specific producer and are part of a wider initiative. For instance, American Family launched an inclusive offer in partnership with Ring: $ 30 discount off the $ 199 Ring Video Doorbell, reimbursement of deductible in case of burglary, and the enrollee may be eligible to receive up to a 5% “Proactive Home Protection Discount” upon installation and activation of the Ring Device (American Family, 2018). A total of 7 premium discounts emerged across the sample analyzed, averaging at $ 105.45 per offer (comprehensive of discount on the device and discount on installation fees, where applicable). As represented in Figure 3, such offers are mostly concerned with safety and fire prevention devices, in accordance with the previous findings on premium discounts.

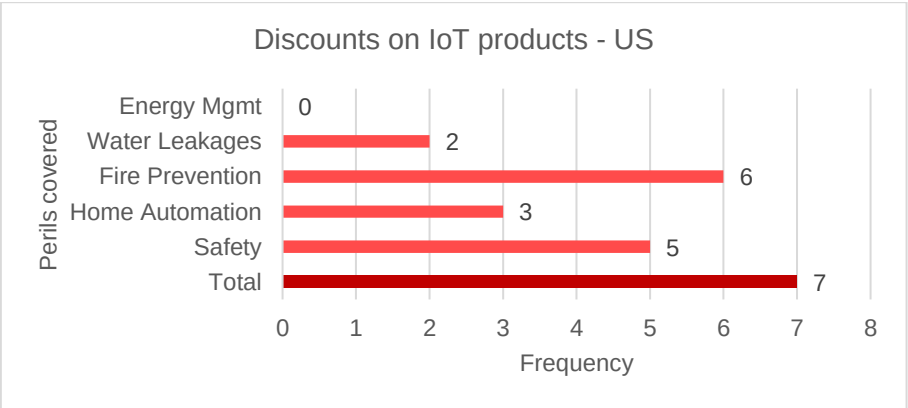

Figure 3 - Peril categories for discounts on IoT products in the United States

Finally, only two **pilot projects** have been identified. One is an additional premium discount applied by Berkshire Hathaway on top of the regular clause for correct installation and maintenance of the connected security system, and the other is a pilot project launched in Minnesota by American Family, offering a free NEST smoke detector (selling at $ 99) combined with a 5% discount on the insurance premium. Even from this preliminary analysis, it is clear that the majority of American insurers are experimenting with smart home policies. However, they are mostly doing so within predetermined boundaries and, in general, the nature of the initiatives does not differ much from one company to another.

Moving to the other side of the Atlantic, the **European Union** presents a more varied landscape, despite IoT-related clauses and initiatives are somewhat less diffused. The EU insurance market is much more fragmented than the United States, and the top 30 P&C insurance companies analyzed make up to only 45% of the total market. Among these, only half of these companies are implementing smart home-related initiatives, for a total of 15 initiatives in place. Hence, a first difference across the two markets emerges: European players are only implementing one initiative at a time, while their American counterparts are more at ease with having up to three initiatives active.

The European landscape also offers a wider variety of initiatives, which can be classified in four different categories. As shown below in Figure 4, platforms are the most common, followed by discounts on IoT products, premium discounts and pilot projects.

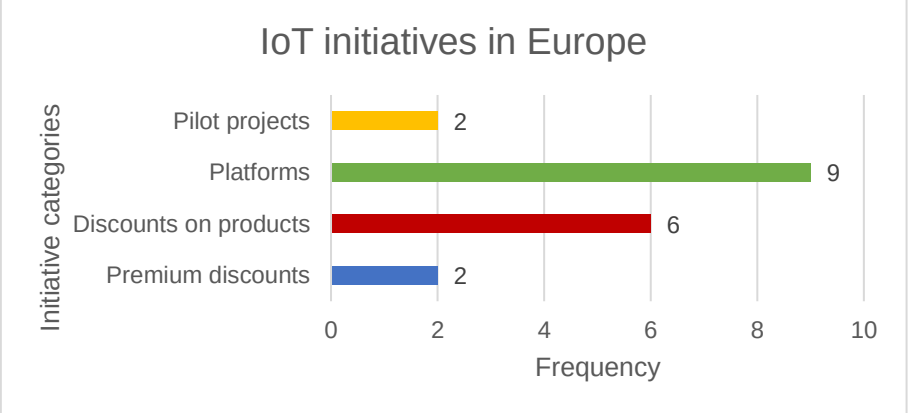

Figure 4 - Different categories of IoT initiatives in Europe

As explained above, **platforms** are defined as an end-to-end smart home solution offered by the insurance provider. They usually consist of a number of sensors of various kinds to be installed in the customer's home, and can wirelessly communicate with one another by means of a central hub (usually in the form of a tablet). Among the European insurers analysed, nearly one out of three has a platform offer in place. Sometimes customers can choose among various versions of the platform, to select the one most suitable to their needs. In Europe, the average cost of a home insurance IoT platform is € 195 per year, and are most common in France and Italy. With respect to the peril categories covered, all the platforms analyzed included some form of safety protection, in the form of alarm systems, intrusion detectors and security cameras which can be controlled remotely from a smartphone app. As shown in Figure 5, other commonly covered peril categories are protection from fire and water leakages, while energy spending and home automation are usually disregarded.

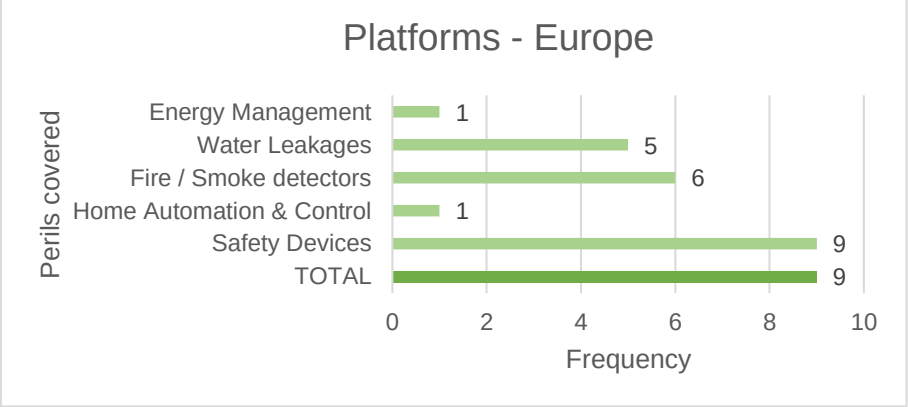

Figure 5 - Peril categories for IoT platforms in Europe

Discounts on IoT products represent the second-preferred category among European insurers. These usually emerge as consequence of a partnership between an insurance provider and an international smart home device manufacturer (such as Philips Hue or Nest), therefore it's quite easy to extend such initiatives in multiple countries. Among the 6 examples identified, two of them come in the form of allowances. As described above, an allowance is how much an insurer is willing to cover for the purchase and installation of a connected alarm system, after the insured party has fallen victim of a burglary. The average discount offered is € 121, slightly

higher than in the United States. On the other hand, the allowances ranged from £ 10,000 (€ 11,435) to £ 15,000 (€ 17,153). As it can be inferred from Figure 6, such offers are mostly concerned with safety devices, followed by water leakage sensors and fire prevention devices, while energy management sensors were completely excluded. Arguably, at the state of the art, these kind of sensors do not provide data that can be directly correlated with the probability of damages.

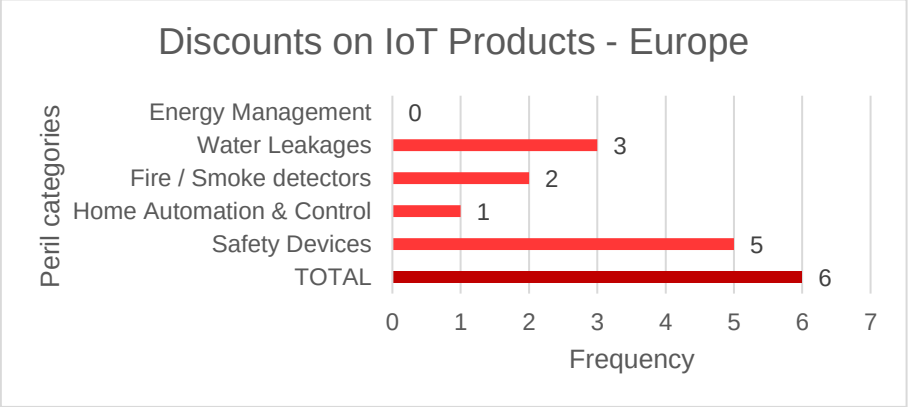

Figure 6 - Peril categories for discounts on IoT devices in Europe

Only 2 **discounts on premiums** have been identified, concerning energy management and safety devices. The first is *EnergieBonus*, a very peculiar initiative launched by Wiener Städtische (Vienna Insurance Group). The offer consists in a premium discount of up to 35 € /month for the installation of energy-saving or energy management devices, for every household with an energy consumption of up to 70 kwH/sqm (Wiener Städtische, 2018). The second is offered by Zurich in the United Kingdom in partnership with Cocoon, an AI-powered security camera system for the home. By purchasing a Cocoon to better protect their home, Zurich UK customers will receive a 10% discount on Zurich's home insurance. In addition, when bought at the same time there will be an exclusive discount of £50 for Zurich customers who purchase a Cocoon (Zurich UK, 2018).

Finally, two **pilot projects** have been highlighted in the European market, launched by Achmea, a Dutch insurance provider, and Société de Groupe D'Assurance Mutuelle Covéa. Achmea is partnering with Accenture to launch *Homies*, a peer-to-peer home

security platform that allows neighbours, friends and family to help each other out in case of fire or burglary. The platform connects innovative home security solutions as Point, Roost, and others to prevailing messaging apps, and is planned to scale to 100,000 households in two years, and costs € 249 all-inclusive (Accenture, 2018). In France, as early as 2013 Covéa launched a customizable fire and/or intrusion alert service provided with the SIGFOX network, for € 79 with a € 3 yearly subscription. It will enable insured customers to be warned directly with an SMS, in case the home installed sensors detect smoke or movement (Covéa, 2018). Despite the fact that it is still unclear whether the project is still in the experimentation phase, it has been categorized as a pilot project because there was no information available concerning its current status.

Correlation Analysis

After a brief exploration of the dataset in Excel, described above, the bulk of the analysis was performed using the SPSS software. The next step was to conduct a **correlation analysis** of the relationships between the financial variables and information concerning IoT initiatives. The goal of such correlation analysis is to lay the foundation for more articulated analyses, by making it possible to identify high-level relationships among the variables.

The **correlation coefficient** shows the strength of the relationship between two variables. 0 means that there is no linear correlation at all between the two variables, 1 indicates that the two variables perfectly move in the same direction, and -1 means that the two variables perfectly move in the opposite direction. In other words, a correlation coefficient of 1 or -1 means that one variable can be expressed as a linear combination of the other and a constant term.

The two datasets were examined separately, as they are related to two very different contexts. After computing pairwise Pearson correlations, these were ranked according to their p-values, i.e. **statistical significance** (two-tailed). Then, correlations displaying a significance value higher than 0.05 were deemed significant, while those displaying a p-value between 0.05 and 0.1 are to be interpreted with more caution,

despite being still significant. Correlations with a p-value higher than 0.1 were discarded.

Concerning the **US**, the most significant correlations are displayed in Table 1.

Variable 1	Variable 2	Correlation coefficient	Significance (two-tail)
Market_share_US	Purchase_US	**0,538**	0,005
Market_share_US	Pilot_US	**0,523**	0,007
Market_share_US	Purchase_maxamount_US	**0,51**	0,009
Expense_ratio_US	Initiative_US	**-0,492**	0,012
Expense_ratio_US	Init_safety_US	**-0,492**	0,012
Expense_ratio_US	Discount_maxamount_US	**-0,496**	0,012
Loss_Ratio_US	Initiative_US	**0,483**	0,014
Loss_Ratio_US	Init_safety_US	**0,483**	0,014
Market_share_US	Discount_maxamount_US	**0,467**	0,019
Expense_ratio_US	Discount_US	**-0,457**	0,022
Market_share_US	Total_coverage_US	**0,455**	0,022
Loss_Ratio_US	Discount_US	**0,454**	0,023
Combined_Ratio_US	Init_energy_US	**0,432**	0,031
Market_share_US	Init_energy_US	**0,43**	0,032
Market_share_US	Initiative_US	**0,408**	0,043
Market_share_US	Init_safety_US	**0,408**	0,043
Market_share_US	Init_control_US	**0,406**	0,044
Market_share_US	Discount_US	**0,382**	0,06
Expense_ratio_US	Init_water_US	**-0,03**	0,0885
Combined_Ratio_US	Pilot_US	**0,339**	0,098

Table 1 - Significant Correlations (United States)

Starting from the most significant correlations, a strong positive association has been discovered between an **insurer's market share** and IoT initiatives, particularly in relation to discounts for purchase of devices, pilot projects, amount of discount offered (both for premiums and devices) and, to a lesser extent, safety, control and energy initiatives. This phenomenon demonstrates that larger players are more likely to implement such initiatives and are keener on experimenting on unconventional policies – see the strong positive correlation with pilot projects.

Only a few insights have been gathered concerning the **combined ratio**, namely a positive association with energy-related initiatives and a less significant association with pilot projects. This can be explained in two possible ways: either insurers implementing such initiatives are more likely to be less profitable than their peers, or players with stronger pressure on their revenues have been keener to experiment with unconventional policies as a mean to improve their condition. It's always worth remembering, however, that these results may be a statistical artifact generated by the sample under investigation.

The most interesting part of the analysis comes by examining the two components of the combined ratio. The **expense ratio** shows a consistent negative correlation with respect to safety initiatives, the presence and amount of premium discounts and IoT initiatives in general. This is a strong argument in support of the second of our hypotheses: IoT makes it much easier to verify the rightness of a claim after an incident has occurred, hence a lower expense ratio. On the other hand, the **loss ratio** seems to increase with connected home initiatives, especially discounts and initiatives connected to safety devices.

The **European landscape** seems much more blurred, as the correlations identified were substantially less meaningful with respect to the United States. The most significant ones are presented in Table 2. Interestingly, only direct correlations occurred.

Variable 1	Variable 2	Correlation coefficient	Significance (two-tail)
LOSS-RATIO	Init_safety	**0,467**	0,009
COMBINED_RATIO	Initiative	**0,448**	0,013
LOSS-RATIO	Init_coverage	**0,408**	0,025
COMBINED_RATIO	Allowance_amount	**0,39**	0,033
Market_share	Purchase_amount	**0,378**	0,04
LOSS-RATIO	Initiative	**0,368**	0,045
COMBINED_RATIO	Init_safety	**0,366**	0,047
GWP_P&C	Purchase_amount	**0,378**	0,064
LOSS-RATIO	Platform	**0,335**	0,07
COMBINED_RATIO	Pilot	**0,326**	0,079

Table 2 - Significant correlations (Europe)

On a general level, it emerged that IoT-related initiatives are **positively correlated with loss ratios** and, consequently, **combined ratios**. As highlighted above, this finding seems counterintuitive, as a higher loss ratio implies that more claims are being paid with respect to gross written premiums, and a higher combined ratio is a sign of lower profitability. Also, the number of perils covered by an initiative seems to have a positive effect on loss ratios, too. No significant correlations were found with respect to the expense ratio, meaning that the relationship between IoT initiatives and insurers' **expense ratio** is still **unclear** in Europe.

At a more granular level, the kind of initiatives which appear to have a higher impact on the loss ratio (and combined ratio) are **safety initiatives**. However, this may as well be due to the fact that burglary prevention initiatives are the most widespread across European Countries (see Figure 5 and 6). Moreover, allowances seem to positively affect the combined ratio. Consistently with the United States, larger players are more likely to launch initiatives related to purchase of smart home devices, offering a larger discount – see the positive relationship between the market share and the variable "Purchase_amount".

Three other positive relationships were found, but they need to be interpreted with more caution as their p-levels exceed 0.05. Namely, the link between gross written premiums and the discount on IoT purchases, the relationship between loss ratios and platform initiatives, and the one between combined ratios and pilot projects.

Factor and Regression Analysis

After studying the most significant correlations in the two datasets, the second step was to perform a regression analysis, with the aim of creating a model for the above-described relationships. However, it was not possible to come up with a significant model by performing a linear regression analysis on the raw variables. In fact, the sample sizes were quite limited, with a consistent endogeneity among the variables describing the initiatives.

To overcome this issue, a **factor analysis** was performed on the two datasets, to obtain a limited number of factors that would capture most of the information conveyed by the descriptive variables, and at the same time reduce collinearity consistently.

Factors were extracted among the variables of interest (from Exhibit 2, from Initiative to Pilot) by applying Principal Component Analysis as extraction method. Such factors have been used as dependent variables for linear (OLS) regressions, in an attempt to explain the financial variables.

Concerning the **United States** database, the factors extracted accounted for around 90% of the variation of the individual variables – see Exhibit 3 for the table of extracted communalities). The least explained variable was Init_Water_US, for which 71.8% of the variation was captured. According to the eigenvalue role and the elbow point in the scree plot, **four factors** were extracted accounting for 90.8% of total variance – see Exhibit 4.

The matrix of loadings has been rotated according to the varimax method (with Kaiser normalization) to ease the interpretation of the factors, as highlighted in Table 3 below.

Variables	Component			
	1	2	3	4
Initiative_US	0.937			
Total_coverage_US	0.571	0.47	0.669	
Init_Safety_US	0.937			
Init_Control_US			0.906	
Init_Fire_US	0.595		0.606	-0.341
Init_Water_US		0.694	0.455	
Discount_US	0.964			
Discount_maxamount_US	0.843			0.467
Init_Energy_US		0.926		
Purchase_maxamount_US				0.954
Purchase_US		0.386	0.486	0.73
Pilot_US		0.912		

Table 3 - Matrix of rotated loadings (United States)

In the table, only loadings greater than 0.3 are shown. The components have been interpreted as follows:

- Component 1 – "***Basic Initiatives***", captures discounts, fire and safety initiatives, i.e. the most common in the market.
- Component 2 – "***Experimental Initiatives***" comprehends more unconventional initiatives, such as pilot projects and those involving energy management and water leakage devices.
- Component 3 – "***Breadth of the Initiative***", encompassing initiative coverage and categories beyond the "basic" ones involving safety.
- Component 4 – "***Monetary Incentive***", capturing the amounts of premium- and devices discounts and purchase initiatives, which depend heavily on monetary incentives offered to the customer.

The above factors have been used as independent variables in linear regression models, in an attempt to model their relationship with the financial indicators. The results are displayed in the following paragraphs.

First, the **loss ratio** was regressed against factors, but only its relationship with factor 1 (Basic Initiatives) was found significant at the 5% level. The resulting model has an R-square of 0.225 adjusted to 0.191, which is quite remarkable for a single regressor. As described in Exhibit 5, the relationship between loss ratio and Basic Initiatives can be modelled as follows:

$$\boldsymbol{Loss\ Ratio} = const. + 0.387 * Basic\ Initiatives + \varepsilon$$

The model of **expense ratio** against Basic Initiatives and Monetary Incentives is significant at the 5% level, with an R-square of 0.288 adjusted to 0.224. As shown in Exhibit 6, unfortunately the coefficient for Monetary Incentives is not significant, and needs to be interpreted with caution. The relationship can thus be modelled as follows:

$$\boldsymbol{Expense\ Ratio} = const. - 0.512 * Basic\ Initiatives - 0.162 * Monetary\ Incentives + \varepsilon$$

The **combined ratio** was regressed against factors 2 and 4 – Experimental Initiatives and Monetary Incentives, and the model is significant at 10% level. The adjusted R-square is quite low, at 0.125, consistently with the previous findings concerning

correlations. Similarly to the expense ratio model, the coefficient for Monetary Incentives was not significant, but to a lesser extent. Please refer to Exhibit 7 for the model specificities.

$$\boldsymbol{Combined\ Ratio} = const. + 0.385 * Exper.Initiatives - 0.222 * Monetary\ Incentives + \varepsilon$$

Finally, the **market share** was regressed against Basic Initiatives, Experimental Initiatives and Monetary Incentives. The model was significant at the 1% level, with an adjusted R-square of 0.356. As displayed in Exhibit 8, the coefficients were significant at the 10% and 5% level. The relationship can therefore be modelled as follows:

$$\boldsymbol{Market\ Share} = const. + 0.298 * Basic\ Initiatives + 0.372 * Experimental\ Initiatives + 0.458 * Monetary\ Incentives + \varepsilon$$

Concerning the **European** landscape, the components extracted accounted for an average of 78% of the individual variables' variation, as shown in Exhibit 9. The least captured ones were Platform_cost and Init_control, at 0.549 and 0.416 respectively. Consistently with the United States, our factors were extracted according to the eigenvalue rule and the scree plot, accounting for 78.18% of total variance. Please refer to Exhibit 10 for the table of initial eigenvalues and extracted factors.

The matrix of rotated loadings, for which only the absolute values greater than 0.3 are shown, is reported below in Table 4.

Variables	Component			
	1	2	3	4
Initiative	0,819			
Init_coverage	0,673	0,676		
Init_safety		0,8		0,481
Init_control	0,597			
Init_fire	0,496	0,637		

Init_water	0,869			
Init_energy			0,88	
Discount			0,95	
Discount_maxamount			0,998	
Purchase	0,888			
Purchase_amount	0,847			
Allowance_amount				0,961
Platform	0,338	0,841		
Platform_cost	0,423	0,598		
Pilot	-0,33	0,702		

The factors highlighted in Europe are much more specific than their American counterparts, and have been interpreted according to the most frequent initiative characteristics:

- Component 1 – "***Initiative Breadth***", capturing a wide array of initiative features, purchase-related characteristics and, to a lesser extent, platforms.
- Component 2 – "***Safety Platforms"***, involving platform characteristics, safety- and fire-related initiatives.
- Component 3 – "***Energy Discounts"***, encompassing energy initiatives, discounts and their amount.
- Component 4 – "***Safety Allowances***", capturing allowance amounts and, to a lesser extent, safety initiatives. This may be considered an ad-hoc factor, considering that all the allowances identified were safety-related.

Following the same procedure described above, these factors were used as independent variables in linear OLS regression models for financial indicators.

The linear regression model for **loss ratio** against factors 2 and 4 (Safety Platforms and Safety Allowances, respectively) is significant at the 5% level, with an R-square of 0.236, adjusted to 0.179. The specifics of the regression can be found in Exhibit 11. The coefficients for both regressors are significant at the 5% and 10% level respectively, and the model can be described as follows:

$$\boldsymbol{Loss\ Ratio} = const. - 0.362 * Safety\ Platforms - 0.324 * Safety\ Allowances + \varepsilon$$

The regression of the **expense ratio** against the factor did not reach a satisfactory significance level, and has been **excluded** from the analysis. However, such an outcome is not surprising: from the correlation analysis, no meaningful results emerged concerning the relationship between the expense ratio and the variables relating to the initiatives.

The **combined ratio** was regressed against the same factors used to compute the loss ratio (Safety Platforms and Safety Allowances), and the resulting model is significant at the 5% level. Expectedly, the R-squares are slightly lower, as it's necessary to take into account the variation brought by the expense ratio – which cannot be accounted for. The first coefficient is slightly beyond the 10% level (0.109), while the second is well below the threshold. According to Exhibit 12, the resulting model can be described as follows:

$$\boldsymbol{Combined\ Ratio} = const. - 0.285 * Safety\ Platforms - 0.347 * Safety\ Allowances + \varepsilon$$

Finally, the model of the market share against factors was not found significant, for any combination of regressors. According to the same phenomenon concerning the expense ratio, the indicator shows relevant correlations only with respect to one variable, and finding a satisfactory model was therefore quite unlikely.

Limitations of this study

As highlighted in the previous sections, the results of this analysis need to be interpreted with caution, for the following reasons:

- The **number of observations** is quite low, especially when compared to the number of variables. In fact, the American and European datasets are composed by 25 and 30 observations respectively, and cannot be merged as they relate to different phenomena.
- Most variables regarding the initiatives were derived from policy contracts, i.e. qualitative sources. Hence, the resulting variables were **binary categorical** ("dummy"), which may not accurately represent nuanced phenomena.

- No statistical devices could be found to remove or mitigate the impact of **endogeneity** on the dataset, as no instrumental variables were available.
- The **financial data** used for the analysis was not updated to the last financial year, as a significant portion of the companies analyzed had not published their 2017 financial statements at the time of data collection. Hence, the analysis may be overly influenced by 2016 trends and the most recently launched initiatives may not be accounted for. Some out-of-sample analysis should therefore be performed in order to further confirm the conclusions of this study. An ideal analysis should be carried out over several years, adding all the initiatives launched and excluding the ones dismissed each year.
- **Profitability of home insurance players** depends on a high number of factors beyond the scope of this study. To name a few, underwriting income is extremely sensitive to weather-related events (hurricanes, hailstorms, tornados, harsh winters), neighborhood crime and competition in the market.

Results

The **frequency analysis** highlighted the following insights:

- **Market maturity**: from a frequency perspective, the American market for IoT home insurance policies seems more developed than the European one, with a grand average of 0.92 initiatives per insurer against 0.5 in the EU. The average initiative coverage is 2.29 in the US, while in Europe it stops at 1.3. However, players in the Old Continent are implementing a wider range of initiative typologies, while American initiatives seem much more “standard”.
- **Initiatives per insurer**: companies active in the European market tend to implement only one initiative at a time, while their American counterparts may carry out up to 3 initiatives at the same time.
- **Most frequent categories**: the perils most frequently covered are quite homogeneous across the two markets. Safety initiatives rank first, followed by Fire and, to a lesser extent, Water. This is quite surprising, considering that water-related damages represent the most frequently filed insurance claim among home insurers, and about 20% of all insurance claims are relate to some

kind of water damage. Such a finding gains even more relevance, considering that 93% of all water damages can be prevented (Arguello, Hope and Associates, PLLC, 2013). One may argue that state-of-the-art water leakage sensors are very expensive and not much diffused, so it would make little sense to design ad-hoc policies for them. In addition, events such as burglaries or break-ins are much more traumatic for the victims than a burst pipe, and insurers can capitalize on providing their customers with a feeling of safety.

- **Amount of discount**: it emerged that premium discounts offered were larger in Europe, averaging at 14% (against 11% in the US, considering the reference year and the sample analysed). This seems to support the theory that the American market is closer to maturity, with more standardized clauses and offers. However, American insurers offer more conspicuous advantages concerning the purchase of IoT devices, with a medium discount of USD 626 (considering discounts on installation fees).

Moving forward, the **correlation analysis** revealed clearer relationship patterns among American insurers, while the European landscape appears more blurred. This may partially be explained by the lower homogeneity of the European market, where stronger regional differences introduce a higher variance, making it more difficult to find statistically significant results. In particular, the following insights can be gathered:

- Strong evidences for **market share effect** were found in the United States, especially concerning purchase initiatives and pilot projects. However, such effect was only marginal in the European setting. A possible explanation may lie in the lower market concentration, and stronger fragmentation due to geographical and legislative borders may also play a role.
- In the US, a strong negative linear correlation was observed between the **expense ratio and IoT initiatives**, while this was not the case in Europe.
- In both markets, IoT initiatives may seem to have **a direct impact on the loss ratio** and, to a lesser extent, on the **combined ratio**, thus implying a decrease in profitability. Again, these relationships are more pronounced in the American setting. However interesting and counterintuitive, these trends need to be validated by further analysis before being discussed: in fact, it is plausible that

decreased profitability may incentivize companies to launch innovative policies, and not the other way around.

Finally, a **factor** and **regression analysis** was performed to validate these findings, with the following outcomes:

- The **market share effect** observed in the US was confirmed, with the model accounting for a significant proportion of the indicator's variance (35.6%).
- The negative relationship between **initiatives and the expense ratio** among American insurers was confirmed as well, especially in connection with basic initiatives, partly validating the initial hypothesis.
- With respect to the **loss ratio**, its positive relationship with IoT initiatives was only confirmed in the American setting. In contrast, in Europe the regression model highlighted a negative relationship with Safety Platforms and Safety Alliances, in accordance with our hypothesis.
- Finally, the **net effect** of IoT initiatives **on the combined ratio** was negative in Europe, and unclear in the United States (the overall model is significant, but the two regressors have opposite sign). As expected, the R-squares are significantly lower for the combined ratio, as it's necessary to account for the variation in both its individual components.

Discussion

Hypothesis verification

As shown in Figure 7 below, **all four hypotheses have yielded significant models in at least one market** out of two. Hypothesis 4 was not present in the original set of hypotheses but was added after the explorative analysis, as it may yield interesting insights about the underlying structure of the two insurance markets and their relative fragmentation. In the list of regressors, the ones that were borderline significative are reported in brackets.

Hypothesis	European Union	Sig.	R^2	United States	Sig.	R^2
H1. - *Companies implementing smart home insurance initiatives present, on average, a* ***lower expense ratio***	✗ Not verified	-	-	✓ Verified, depending on: • Basic Initiatives • (Monetary Inc.)	0.024	0.288
H2. - *Companies implementing smart home insurance initiatives present, on average, a* ***lower loss ratio***	✓ Verified, depending on: • Safety Platforms • Safety Allowances	0.026	0.236	✓ Verified, depending on: • Basic Initiatives	0.016	0.225
H3. - *Companies implementing smart home insurance initiatives present, on average, a* ***lower combined ratio***	✓ Verified, depending on: • Safety Allowances • (Safety Platforms)	0.048	0.202	✓ Verified, depending on: • Exper. Initiatives • (Monetary Inc.)	0.049	0.198
H4. (Additional) - *Larger companies are more likely to implement IoT Initiatives –* ***market share effect***	✗ Not verified	-	-	✓ Verified, depending on: • Basic Initiatives • Exper. Initiatives • Monetary Incentives	0.006	0.437

Figure 7 – Model significance

Moving to the verification of the hypotheses above, the overall view can be found in Figure 8 below. **The analysis confirmed Hypotheses 1** and **4**, even if only in relation to the American market. Indeed, the United States present a much more uniform insurance market in comparison to the EU, with a homogeneous legislative framework, less fragmentation and more consistent best practices. In particular, the market share effect presented in Hypothesis 4 is deeply influenced by the underlying structure of the market, while the expense ratio investigated in Hypothesis 1 may be a result of industry practices and investigation routines.

Hypothesis 2, relating to the **loss ratio**, was not verified in any of the two markets. Namely, it **seems to increase with the implementation of IoT initiatives**, especially

the most basic ones (in the US) and those relating to safety issues (in Europe). Such a conclusion is very robust but, at the same time, quite unexpected. In addition to the possible explanations stated above, this phenomenon may arise from the fact some loss events can now be traced and reported with an increasing level of detail, making it easier to gather evidence to file an insurance claim. For example, it's easier to provide proof of a burglary or an arson, if the house is equipped with a connected safety system and security cameras. Indeed, the fact that IoT may make it easier for homeowners to report loss events and file claims should be investigated by future research. To examine the phenomenon, it would be interesting to analyze the number of claims, the expenses related to such claims, and the percentage of rejected claims before and after the implementation of an IoT initiative. However, such data may not be readily available: unless an initiative is launched at the beginning of the financial year, it's not straightforward to obtain the revenue breakdown before and after the launch. Moreover, usually the information relating to rejected claims is not available to the public.

Moving to **Hypothesis 3**, concerning the combined ratio, the landscape gets more blurred. In Europe, the **relationship between safety initiatives and** the **combined ratio** is definitely positive, following the trend observed with respect to the loss ratio. Thus, the hypothesis is clearly rejected in the European setting. However, in the United States the direction of the relationship is uncertain: the combined ratio increases with Experimental Initiatives, but decreases with Monetary Incentives. Interestingly, the factor for Experimental Initiatives did not appear in the models used to define the two components of the combined ratio. Indeed, the combined ratio is a very complex indicator that depends on many phenomena, and analyzing it as the sum of its component may be overly simplistic.

In light of the above, **we can conclude that**:

- In the United States, IoT initiatives are associated with lower verification, fees and fraud investigation expenses (**lower expense ratio**);
- In both markets, Basic and Safety home insurance initiatives are related to higher claim-related expenses and refunds (**higher loss ratio**);

- In Europe, the implementation IoT initiatives is related to lower overall profitability along the homeowners' lines (**higher combined ratio**), while in the United States the global effect is unclear; Finally, it has been demonstrated that larger insurance players in the United States are more likely to implement smart home initiatives (**market share effect**).

Hypothesis	European Union	Sig.	R^2	United States	Sig.	R^2
H1. - *Companies implementing smart home insurance initiatives present, on average, a* ***lower expense ratio***	✗ No information	-	-	✓ Decreasing with: • Basic Initiatives • Monetary Inc.	0.024	0.288
H2. - *Companies implementing smart home insurance initiatives present, on average, a* ***lower loss ratio***	↻ Increasing with: • Safety Platforms • Safety Allowances	0.026	0.236	↻ Increasing with • Basic Initiatives	0.016	0.225
H3. - *Companies implementing smart home insurance initiatives present, on average, a* ***lower combined ratio***	↻ Increasing with: • Safety Allowances • Safety Platforms	0.048	0.202	? Uncertain: • Increasing with Exper. Initiatives • Decreasing with Monetary Inc.	0.049	0.198
H4. (Additional) - *Larger companies are more likely to implement IoT Initiatives –* ***market share effect***	✗ No information	-	-	✓ Increasing with: • Basic Initiatives • Exper. Initiatives • Monetary Incentives	0.006	0.437

Figure 8 - Hypotheses verification

Implications for the relationship with insurance companies and their customers

At present, for most consumers, insurance is a grudge purpose: they buy it hoping they will never use it, often because it's mandatory, frequently switching providers at renewal time if they find more convenient offers. But as seen above, IoT is bound to change the very nature of risk assessment, shifting from an *a-priori* to a *dynamic* assessment throughout the whole policy period, making use of predictive analytics techniques. Therefore, the more data insurers are able to collect about a given customer, the more accurate risk predictions will be, leading to more efficient and fair pricing. Such desirable outcomes can only be achieved by strengthening existing consumer relationships and prolonging the average subscription period. Now more

than ever, creating positive **consumer engagement** is crucial for the successful introduction of Smart Home insurance policies.

One way to increase customer engagement is to encourage customers to **improve their behaviour** thanks to the increased possibilities for tracking and data gathering. The trend of the **Quantified Self Movement** is increasingly visible in consumer markets, and is especially solid in relation to activity and fitness trackers (Marcengo, 2014). However, oftentimes such behavior is not oriented towards a specific purpose. Rather, it grows into a form of lifelogging, a way of collecting data as a sort of game with an end in itself. This phenomenon is likely to expand to the field of the Smart Home, as customers will increasingly have the possibility to monitor energy consumption patterns, indoor temperature, usage rate of single appliances, water expenditure and so forth. Thus, insurers should exploit the opportunity to give this data collection a tangible meaning, by allowing users to **save money on their policies** and obtain a level of service more suitable to their individual needs.

Ultimately, insurers need to redesign their **customer service and customer relationship management practices** around the concepts of prevention and dynamic risk assessment. Up to now, unless they suffer a burglary or an accident, customers only speak to their insurer upon renewal. Current customer service is designed around the annual lifecycle, or focused around the event of the accident and the subsequent claim settlement. Indeed, the lack of consumer engagement can be traced back to the **intangible nature** of insurance products: if all goes well, insurance expenses are "wasted" money for the insured, who in the normal course of events would never have the chance to verify how good the underlying coverage is (Solomon, 2017).

At present, customer service agents require new skills, processes will have to be redesigned and information made available to ensure customer experience is tailored to the **different needs of IoT consumers**. Compared to traditional policyholders, IoT consumers expect technological innovation to be backed up by integrated customer service across **multiple channels**: traditional channels, online and mobile platforms. However, many service providers still struggle to bridge silos between different touchpoints, who are all responsible for individual parts of the customer journey

(Rawson, Duncan, & Jones, 2013). To be credible in a digital world, seamless integration across channels at every step of the customer journey is a prerequisite.

The future of home insurance

The combination of literature review and quantitative analysis has provided a complex but fairly detailed picture of what the business model of home insurance might look like a few years from now, and its possible implications on insurers' profitability and the relationship with their customers.

To validate and refine this picture, a number of **professionals and consultants** in the fields of Property Insurance, Insurtech, Data Security and Smart Home providers has been interviewed on the matter, during the months of March and April 2018. The full list of interviewees can be found in Exhibit 13.

All the respondents highlighted the presence of strong synergies between Smart Home providers and insurers, provided that the latter have **clear objectives on the kind of data** they are interested in, and are aware of the questions this data should be able to answer. As highlighted by **Michele Treglia**, Insurtech Consultant in Turin, Italy, data collection should be perceived not as an end in itself, but as a mean to help the company to achieve its future objectives. Therefore, insurers must first identify what are the needs of the client relative to a given IoT system or device (for example, to detect water leakages before damages occur). Only then can insurers identify the kind of data required to provide a specific solution (in our example, what is the condition of the pipes in critical areas, the pressure of the water, and if maintenance has been done). Once identified, such guidelines should lead insurance companies in **crafting their IoT strategy**, data collection and prioritization decisions – i.e., what data to analyze, what data to keep, and what data to discard.

At present, however, many professionals feel insurance players have no clear strategic direction, but are experimenting different solutions while trying to make a sense of what is going on in the market. Among them **Craig Polley**, Director at Digital Risk Services Limited in London: "*it's important to understand that the industry is leveraging IoT and IoE* (Internet of Everything) *purely for marketing purposes. This means they are not*

applying new actuarial or underwriting methods modelled on data acquisition or telemetry from sensors in the home. Likely, a third-party will capture data, and make use of it".

Indeed, it's very time-consuming for traditional property and casualty insurers to develop internally all the capabilities required to rapidly **scale up to IoT data volumes**, in terms of capacity, cutting-edge IT ecosystem and analytics. Moreover, it's very difficult to subsidize the cost of equipment, backhaul, IT infrastructure, storage and ad-hoc data analysts. As confirmed by our data, insurers typically operate on **thin margins**: the average combined ratio in 2016 was 96.1% among the top US insurers, while in Europe it reached 96.7%. This leaves companies with operating margins of 3.9% and 3.3% respectively, meaning large IT investments need to be planned well in advance. In addition, companies are struggling to maintain long-term relationships with their clients because of **fierce price competition**. Finally, as uncertainty is deeply embedded in their business model, they are required to keep a fraction of their earnings frozen as **cash reserves**, in case of unexpected contingencies or unforeseen expenses.

From the interviews, it emerged that in general traditional insurers are **not ready** to address the issues of storage, analysis and responsible management of data: therefore, the most logical conclusion is to **outsource** these functions to third parties. To do so, insurance players should first develop a **clear partnering strategy** and define critical control points (to name one, the issue of data ownership). Then, they can identify and evaluate potential partners, establish a strong partnership network, and create ecosystems built on this foundation. The most viable solutions seem to be **SaaS** (Software-As-A-Service) or **PaaS** (Platform-As-A-Service). They are less costly than conventional solutions, and pay-as-you-go models allow businesses to pay only for what they are using and not spend on unused licenses. Moreover, it's easier to scale up to IoT volumes, as the IT infrastructure is managed by the vendor, which has to guarantee a specified level of service. An example cited by one of the interviewees is Neos, a British company offering digital solutions for players in insurance, financial and information services.

To conclude, **Valentino Ricciardi** from McKinsey highlighted that insurers need to make themselves attractive to potential partners, by considering carefully how to position themselves within an IoT ecosystem. For example, private customers are increasingly suspicious of companies collecting their data, thus insurers can present themselves as trusted and reliable collaborators by highlighting their capabilities in **risk assessment**. Indeed, there is a very thin line between "creepy" and "cool" when it comes to IoT. The interviewee pointed out that "*a lot of the concern comes from distrust and a lack of transparency about what is being used and why, but all the research shows that customers tend to not worry about these things as much if they believe* ***the value equation is in their favor****—if they're getting more for that sacrifice of privacy than they're giving up in the information they're generating*". Insurers are probably not best known for providing a ton of transparency into the rating, underwriting and pricing variables they use, and adopting an IoT-driven structure would be a big step forward in terms of transparency.

Conclusion

In the first section of this Thesis, it is described how the Smart Home phenomenon is likely to disrupt the Property and Casualty insurance sector, by making it possible to shift **from an *ex-ante* to a *dynamic* risk assessment**. Therefore, IoT data is bound to become a critical asset for insurance companies, that need to acquire data analysis capabilities, ensure protection from cyberattacks and, ultimately, build a trust relationship with their customers by providing them with tangible benefits and an increased level of tailored service. In the coming years, insurers will likely offer their customers increasingly personalized policies, changing their mode of interaction to an ongoing relationship, spanning across multiple channels and based upon mutual engagement.

Then, in the second part of the work, the relationship between smart home-related initiatives implemented by European and American insurers has been analyzed, based on a number of **financial indicators**. The data has been analyzed by means of a correlation, regression and factor analysis - the latter was necessary to control for endogeneity among the variables. It emerged that IoT initiatives are associated to a

lower expense ratio, but at the same time with a higher loss ratio. Hence, smart home-related initiatives seem to bring about **more claims**, but it's **less costly to assess such claims**. In Europe, the combination of these two effects brings to a **decreased profitability**, while in the United States the overall effect on the bottom line is unclear. The market share effect was particularly strong in the US, meaning that larger players more likely to implement smart home initiatives.

Overall, there is substantial evidence of an increased availability of **information** that, in accordance with traditional economic theory, **lowers the deadweight loss** (defined as allocative inefficiency, in our case arising from adverse selection and moral hazard) and **erodes the incumbents' profits** (Maskin & Tirole, 1988).

In light of this analysis, one may expect the home insurance industry to **change radically in the next decade**, particularly in relation to the following issues:

- First, the **composition** of the industry itself will be more diverse, as the entire business world is digitizing and breaking down industry barriers. There are likely to be companies from other industries that may also be vying to help reduce risk for customers. Some of these competitors, such as producers of smart appliances or technology companies (e.g. Google or Amazon) may be better positioned within the data value chain. From the results of this analysis, one might expect a **higher industry concentration** as a consequence of the market share effect. However, this phenomenon needs further investigation, as it was only verified in the American market. Overall, to be successful, insurers will need to be more open to partnerships and better at collaborating with companies that have access to more comprehensive sources of data.
- Concerning the **cost structure** of future insurance players, **verification fees** and **internal processing costs** will account for a **smaller and smaller portion** of an insurer's expenses. Data and analytics will be increasingly be employed to automate and enhance processes to handle claims: rather than contacting clients directly, data from IoT devices can provide insights about the series of events preceding an accident. This would also require less personnel to perform such operational tasks, enabling them to dedicate more time to value-added activities, such as customer relationship management. The near totality of

expenses is therefore expected to come from **actual claims settlement**. According to this analysis, future home insurance players may face a **larger number of claims**. However, the near totality of these claims will be genuine: as a matter of fact, IoT makes it harder for the insured to misrepresent facts and inflate claims, as data concerning the loss event will be easily retrieved from the system for verification.

- The inclusion of sensor data in insurance policies will bring **about increased transparency** in the pricing process, a more efficient allocation of surplus and wider implications on society at large. As discussed above, increased monitoring enabled by IoT allows for more accurate risk evaluation, reducing both the impact of adverse selection and the incentives for moral hazard. This would lead to **less unforeseen expenses** incurred by the insurer (less insurance frauds and less need to set aside contingency sums to cover for claims investigation), allowing to decrease premiums for low-risk customers. In a nutshell, the good risk will still subsidize the poor risk, but the gap between the good and the bad will be much closer.
- Finally, the underlying concept of insurance will shift **from cure to prevention**. From a theoretical perspective, IoT allows insurance providers to evolve from being simply payers of claims to valued partners that help their customers monitor, mitigate and avoid risk. For some insurers, this will lead to transformed customer relationships, entirely new sources of customer value and revenue from **hybrid product/services**, **usage-based** insurance and **bundles**. For example, it is not daring to expect insurance policies that automatically adjust based on the time the inhabitants spend in the home, or a comprehensive bundle of car, home and health insurance based on data from the vehicle, connected home appliances and wearable devices.

It is clearly unrealistic to expect that the IoT will remove risk completely. As we have seen, risk will undoubtedly shift **from the physical towards the virtual world**. In fact, connected devices will reduce much of the current peril, that comes largely as a result of negligence and human error. The connected home, anticipated by the imminent arrival of the connected car, will see a shift toward more responsible

customer behaviors, which can now be quantified, measured and accounted for. This is likely to have a positive social impact and strengthen the institutional role of the insurer, from a payer of claims to a proactive risk manager providing tailored advice. Hence, insurance is set to become less a protection against the past and more a warranty for the future.

Exhibits

Exhibit 1 – List of insurance companies considered

United States		Europe	
ID	**Company**	**ID**	**Company**
US_1	State Farm Group	EU_1	Allianz
US_2	Berkshire Hathaway Group	EU_2	Axa
US_3	Liberty Mutual Group	EU_3	Lloyd's
US_4	Allstate Insurance Group	EU_4	Zurich Insurance Group Ltd
US_5	Progressive Group	EU_5	Chubb Limited
US_6	Travelers Group	EU_6	Assicurazioni Generali
US_7	Chubb Ltd.	EU_7	HDI
US_8	Nationwide Corp. Group	EU_8	Mapfre
US_9	Farmers Ins. Group	EU_9	Achmea
US_10	United Service Automobile Assn Group	EU_10	Société de Groupe D'Assurance Mutuelle Covéa
US_11	American Intl Group	EU_11	Aviva
US_12	Zurich Ins Group	EU_12	RSA Insurance Group
US_13	Hartford Fire & Cas. Group	EU_13	Unipol Gruppo
US_14	C.N.A. Insurance Group	EU_14	R+V Versicherung
US_15	AmTrust NGH Group	EU_15	Groupama
US_16	Tokio Marine Holdings Inc. Group	EU_16	ERGO Versicherungsgruppe
US_17	Auto Owners Group	EU_17	AIG Europe
US_18	American Family Insurance Group	EU_18	Vienna Insurance Group
US_19	Erie Insurance Group	EU_19	HUK-COBURG Haftpflicht-Unterstützungs
US_20	WR Berkley Corp. Group	EU_20	Crédit Agricole Assurances
US_21	American Financial Group	EU_21	Sampo
US_22	Assurant Inc Group	EU_22	Ageas
US_23	Cincinnati Financial Group	EU_23	Direct Line Insurance Group
US_24	XL Amer Group	EU_24	Helvetia Holding
US_25	QBE Insurance Group	EU_25	MS Amlin
		EU_26	QBE European Operations
		EU_27	Grupo Catalana
		EU_28	MACIF
		EU_29	Groupe des Assurances du Credit Mutuel
		EU_30	Bâloise-Holding

Exhibit 2 – List of variables analyzed

United States		Europe	
Variable	**Description**	**Variable**	**Description**
ID_US	Company ID	ID	Company ID
Company_US	Registered company name	Company	Registered company name
Year_ founded_US	Founding year	Year_ founded	Founding year

NWP_P&C_ US	Net written premium attributable to property and casualty for the year 2016 (USD)	NWP_P&C	Net written premium attributable to property and casualty for the year 2016 (EUR)
Loss_Ratio_US	Loss ratio for 2016	Loss_Ratio	Loss ratio for 2016
Expense_Ratio _US	Expense ratio for 2016	Expense_ Ratio	Expense ratio for 2016
Combined_ Ratio_US	Combined ratio for 2016	Combined_ Ratio	Combined ratio for 2016
Market_share _US	Reported P&C market share for the year 2016	Market_ share	Reported P&C market share for the year 2016
Initiative_US	Variable indicating whether the company has IoT-related initiatives in place (binary)	Initiative	Variable indicating whether the company has IoT-related initiatives in place (binary)
Total_coverage US	Number of peril categories covered by the initiative	Country	Country where the initiative is in place (if more than one, Country= Multiple Countries)
Init_safety_US	Initiative concerning safety devices (binary)	Total_ coverage	Number of peril categories covered by the initiative
Init_control_US	Initiative concerning home automation devices (binary)	Init_safety	Initiative concerning safety devices (binary)
Init_fire_US	Initiative concerning fire prevention devices (binary)	Init_control	Initiative concerning home automation devices (binary)
Init_water_US	Initiative concerning water leakage devices (binary)	Init_fire	Initiative concerning fire prevention devices (binary)
Init_energy_US	Initiative concerning energy management devices (binary)	Init_water	Initiative concerning water leakage devices (binary)
Discount_US	Initiative relating to premium discounts (binary)	Init_energy	Initiative concerning energy management devices (binary)
Discount_max amount_US	Maximum discount obtainable under the initiative (% on premium, not combined with other offers)	Discount	Initiative relating to premium discounts (binary)
Purchase_US	Initiative relating to the purchase of IoT devices (binary)	Discount_ maxamount	Maximum discount obtainable under the initiative (% on premium, not combined with other offers)
Purchase_max amount_US	Maximum discount on IoT devices obtainable under the initiative (in USD, not combined with other offers)	Purchase	Initiative relating to the purchase of IoT devices (binary)
Pilot_US	The initiative is a pilot project (binary)	Purchase_ maxamount	Maximum discount on IoT devices obtainable under the initiative (in EUR, not combined with other offers)

	Allowance_ amount	Allowance amount reported in the policy (in EUR, not combined with other offers)
	Platform	Initiative relating to an IoT platform provided by the insurer (binary)
	Platform_ cost	Annual cost for the aforementioned platform to be borne by the customer
	Pilot	The initiative is a pilot project (binary)

Exhibit 3 – Table of extracted communalities (United States)

Variables	Initial	Extraction
Initiative_US	1.000	.961
Total_coverage_US	1.000	.996
Init_Safety_US	1.000	.961
Init_Control_US	1.000	.850
Init_Fire_US	1.000	.864
Init_Water_US	1.000	.718
Discount_US	1.000	.966
Discount_maxamount_US	1.000	.934
Init_Energy_US	1.000	.909
Purchase_maxamount_US	1.000	.957
Purchase_US	1.000	.936
Pilot_US	1.000	.852

Exhibit 4 – Table of initial eigenvalues and extracted factors (United States)

Components	Total	% of Variance	Cumulative %
1	**5.800**	48.332	48.332
2	**2.312**	19.266	67.598
3	**1.676**	13.965	81.563
4	**1.116**	9.296	90.860
5	.465	3.872	94.732
6	.310	2.586	97.317
7	.169	1.410	98.728
8	.096	.800	99.528
9	.039	.326	99.853
10	.018	.147	100.000

11	-2,02E-13	-1,68E-12	100.000
12	-2,38E-13	-1,99E-12	100.000

Exhibit 5 – Regression of Loss Ratio against factors (United States)

Model Summary					
R Square		Adjusted R Square		Std. Error of the Estimate	
0.225		0.191		1,7475%	
ANOVA					
	Sum of Squares	df	Mean Square	F	Sig.
Regression	382.24	1	382.24	6.664	.016
Residual	1319.29	23	57.36		
Total	1701.53	24			
Model					
	Unstandardized Coefficients		Standardized Coefficients	T	Sig.
	B	Std. Error	Beta		
(Constant)	62.596	1.515		41.325	.000
REGR factor score 1 - Basic Initiatives	3.991	1.546	.387	2.581	.016

Exhibit 6 – Regression of Expense Ratio against factors (United States)

Model Summary					
R Square		Adjusted R Square		Std. Error of the Estimate	
.288		.224		6,5657%	
ANOVA					
	Sum of Squares	df	Mean Square	F	Sig.
Regression	384.071	2	192.035	4.455	.024b
Residual	948.383	22	43.108		
Total	1.332.454	24			
Model					

	Unstandardized Coefficients		Standardized Coefficients	T	Sig.
	B	Std. Error	Beta		
(Constant)	33.584	1.313		25.575	.000
REGR factor score 1 - Basic Initiatives	-3.815	1.340	-.512	-2.847	.009
REGR factor score 4 - Monetary Incentives	-1.204	1.340	-.162	-.898	.379

Exhibit 7 – Regression of Combined Ratio against factors (United States)

Model Summary		
R Square	Adjusted R Square	Std. Error of the Estimate
0.198	0.125	5,3904%

ANOVA					
	Sum of Squares	df	Mean Square	F	Sig.
Regression	157.536	2	78.768	2.711	.089
Residual	639.251	22	29.057		
Total	796.786	24			

Model					
	Unstandardized Coefficients		Standardized Coefficients	T	Sig.
	B	Std. Error	Beta		
(Constant)	96.088	1.078		89.128	.000
REGR factor score 2 - Experim. Initiatives	2.219	1.100	.385	2.017	.056
REGR factor score 4 - Monetary Incentives	-1.281	1.100	-.222	-1.164	.257

Exhibit 8 – Regression of Market Share against factors (United States)

Model Summary		
R Square	Adjusted R Square	Std. Error of the Estimate

0.437		0.356		1,7475%	
ANOVA					
	Sum of Squares	df	Mean Square	F	Sig.
Regression	49.691	3	16.564	5.424	.006b
Residual	64.127	21	3.054		
Total	113.819	24			
Model					
	Unstandardized Coefficients		Standardized Coefficients	T	Sig.
	B	Std. Error	Beta		
(Constant)	2.624	.349		7.508	.000
REGR factor score 1 - Basic Initiatives	.649	.357	.298	1.818	.083
REGR factor score 2 - Experim. Initiatives	.809	.357	.372	2.268	.034
REGR factor score 4 - Monetary Incentives	.998	.357	.458	2.797	.011

Exhibit 9 – Table of extracted communalities (Europe)

Variables	Initial	Extraction
Initiative	1.000	.909
Init_coverage	1.000	.953
Init_safety	1.000	.912
Init_control	1.000	.416
Init_fire	1.000	.658
Init_water	1.000	.782
Init_energy	1.000	.786
Discount	1.000	.911
Discount_maxamount	1.000	.999
Purchase	1.000	.825
Purchase_amount	1.000	.739
Allowance_amount	1.000	.937

Platform	1.000	.850
Platform_cost	1.000	.549
Pilot	1.000	.632

Exhibit 10 – Table of initial eigenvalues and extracted factors (Europe)

Components	Total	% of Variance	Cumulative %
1	**5.146**	36.758	36.758
2	**2.800**	19.999	56.757
3	**1.790**	12.788	69.545
4	**1.210**	8.644	78.189
5	.910	6.498	84.687
6	.798	5.699	90.386
7	.524	3.743	94.128
8	.438	3.127	97.255
9	.193	1.378	98.634
10	.129	.920	99.554
11	.061	.434	99.988
12	.002	.012	100.000

Exhibit 11 – Regression of Loss Ratio against factors (Europe)

Model Summary

R Square	Adjusted R Square	Std. Error of the Estimate
.236	.179	7,8139%

ANOVA

	Sum of Squares	df	Mean Square	F	Sig.
Regression	509.408	2	254.704	4.172	.026
Residual	1.648.539	27	61.057		
Total	2.157.947	29			

Coefficients

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	64.090	1.427		44.924	.000

REGR factor score 2 - Safety Platforms	3.125	1.451	.362	2.154	.040
REGR factor score 4 - Safety Allowances	2.793	1.451	.324	1.925	.065

Exhibit 12 – Regression of Combined Ratio against factors (Europe)

Model Summary					
R Square		Adjusted R Square		Std. Error of the Estimate	
.202		.143		6,5413%	
ANOVA					
	Sum of Squares	df	Mean Square	F	Sig.
Regression	292.163	2	146.081	3.414	.048
Residual	1.155.280	27	42.788		
Total	1.447.443	29			
Coefficients					
	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	96.730	1.194		80.995	.000
REGR factor score 2 - Safety Platforms	2.013	1.215	.285	1.657	.109
REGR factor score 4 - Safety Allowances	2.454	1.215	.347	2.021	.053

Exhibit 13 – List of professionals interviewed (March-April 2018)

Name	Title	Company	Field	Date

Craig Polley	Director	Digital Risk Services Limited, London	Data Security	7/03/2018
Valentino Ricciardi	Insurance and Insurtech Consultant	McKinsey & Company, Milan	Strategy Consulting (Insurance)	16/03/2018
Michele Treglia	Insurtech Consultant	Guanxi Srl, Turin	Insurtech	25/03/2018
Cathalijn van Rijmenam	Product Manager Smart Home and IoT	Siemens, Zurich	Smart Home provider	25/03/2018
Nikesh Jathanna	Product Manager Smart Home IoT	Altran Deutschland GmBH, Köln	Smart Home provider	12/04/2018

References

(2018, March 31). Retrieved from World Population Clock: http://www.worldometers.info/world-population/

A. T. Kearney. (2017). "Battle for the Smart Home".

Accenture. (2015). *"The Connected Home: New Opportunities for P&C Insurers".*

Accenture. (2018, March). *Homies.* Retrieved from Accenture Innovation Awards: https://innovation-awards.nl/innovation/homies/

Acquisti, B. L. (2015). "Privacy and human behaviour in the age of information". *Science*.

Acquisti, G. (2005). "Privacy and rationality in individual decision making". *Science*.

Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*.

al., D. e. (2006). Risk Measurement with equivalent utility principles. *Statistics & Decisions*, 1-25.

al., H. e. (2015). "Telematics Systems in Usage-Based Motor Insurance". *ScienceDirect*.

Aldrich, F. K. (2003). "Smart Homes: past, present, and future". In Harper, *"Inside the Smart Home".* Springer.

Allstate. (2018, March). *Rogers Smart Home Monitoring*. Retrieved from Allstate Insurance Group corporate website: https://www.allstate.ca/webpages/property-insurance/rogers-smart-home-monitoring.aspx

Almeida, F. (2017). Benefits, Challenges and Tools of Big Data Management. *Journal of Systems Integration*.

American Association of House Builders. (1984).

American Family. (2018, March). *AMFAM Ring - Terms & Conditions*. Retrieved from American Family Corporate Website: https://myapps.amfam.com/amfamring/#/terms

American Family Corporate Website. (2018, April 1). Retrieved from https://apps.amfam.com/amitforms/nest/index.html#/landing

Arguello, Hope & Associates, PLLC. (n.d.). *Water F.*

Arguello, Hope and Associates, PLLC. (2013). *Water Damage Statistics.*

Arnott, R. a. (1988). "The Basic Analytics of Moral Hazard". *Scandinavian Journal of Economics*, 383-413.

Baker. (1996). "On the Genealogy of Moral hazard" . *Texas Law Review*.

BNP Paribas Cardif Italia. (2018, April 1). Retrieved from Press Release – March 3, 2014: Available at: http://www.bnpparibas.it/en/2014/03/03/bnp-paribas-cardif-wins-golden-circle-award-financial-innovation-habitt/

Boyd, C. (2015). "Critical Questions for Big Data" . *Information, Communication and Society*.

Breckenridge, Farquharson, & Hendson. (2014). “The role of business model analysis in the supervision of insurers”. *Prudential Regulation Authority*.

Cardon, & Hendel. (1998). “Asymmetric Information in Health Insurance: Evidence From the National Health Expenditure Survey”. *Mimeo, Princeton University*.

Chiappori, Salanié, Salanié, & Jullien. (2004). Testing for Asymmetric Information in Insurance Markets. *The Journal of Political Economy*.

Cohn. (12th August 2017). “The American Greed Report: You could be committing insurance fraud. Here’s why you should care” . *CNBC*.

Cohn. (2017). “The American Greed Report: You could be committing insurance fraud. Here’s why you should care". *CNBC*.

Coppola, F. (2018, March 11). *President Trump's Trade Tariffs Signal A New Global Trade War.* Retrieved from Forbes: https://www.forbes.com/sites/francescoppola/2018/03/11/president-trumps-trade-tariffs-signal-a-new-global-trade-war/1/#747376d02b19

Covéa. (2018, February). *MAAF ASSURANCES ET SIGFOX S’ASSOCIENT POUR ASSURER L'HABITAT.* Retrieved from Société D'Assurances Mutuelle Covéa: http://www.maaf.com/sites/default/files/news/documents/sigfox_decembre_2013.pdf

Cukier, M.-S. a. (2013). *“'Big Data - a revolution that will transform how we live, work, and think”.*

Cummins, Smith, Vance, & Derhei, v. (1983). *Risk classification in life insurance.* Kluwer Nijhoff Publishing.

Deuker. (2010). “Addressing the privacy paradox by expanded privacy awareness – the example of context-aware services”.

Dickson, D. C. (2016). *Insurance Risk and Ruin.* Cambridge University Press.

DLA Piper. (2017). *Insurance Sector Trends: 2017 Year End Review and Outlook for 2018.*

European Parliament and Council. (2016). General Data Protection Regulation. *Official Journal of the European Union*.

EY. (2015). *“Cybersecurity and the Internet of Things”.*

Flyverbom. (2014). “Datafication, transparency and trust in the digital domain".

Frees, Meyers, & Cummings. (2011). Predictive Modeling of Multi-Peril Homewoners Insurance. *Casualty Actuarial Society*.

Fundaciòn Mapfre. (2016). *Ranking of the largest European Insurance Groups.*

Hitachi Data Systems. (2016). *"The Internet on wheels and Hitachi, Ltd.".*

IHS Markit. (2016). “The Smart Home: A Look Inside Its Burgeoning Market”.

IHS Markit. (2018). *IoT Trend Watch 2018.* London: IHS Markit.

Insurance Europe. (2013). *The Impact of Insurance Fraud.*

Insurance Information Institute. (2018, April 8). *Background on: Insurance Fraud.* Retrieved from https://www.iii.org/article/background-on-insurance-fraud

International Risk Management Institute (IRMI). (n.d.). *Insurance Glossary.*

ITRC. (2017). *2017 Data Breach Report.* Identity Theft Resource Centre .

Kunreuther, Pauly, & McMorrow. (2013). *Behavioral Economics and Insurance: Improving Decisions in the Most Misunderstood Industry.* Cambridge University Press.

Marcengo, R. (2014). “Visualization of Human Behaviour Data: The Quantified Self". *Telecom Italia and University of Turin*.

Maskin, & Tirole. (1988). A Theory of Dynamic Oligopoly, I: Overview and Quantity Competition with Large Fixed. *Econometrica*, 549-569.

McKinsey. (2017). *"There's no place like connected homes".*

Mills. (2005). “Insurance in a climate of change”. *Science*.

Moody's. (2017, November 22). *Outlook for European insurance industry is stable, despite low rates challenges.* Retrieved from www.moodys.com: https://www.moodys.com/research/Moodys-Outlook-for-European-insurance-industry-is-stable-despite-low--PR_375875

Myers-West, S. (2017). *Data Capitalism: Redefining the Logics of Surveillance and Privacy.* Business & Society.

NAIC. (2016). *2016 TOP 25 GROUPS AND COMPANIES BY COUNTRYWIDE PREMIUM - Homeowners Multiple Peril.*

Nance, C. (2003). *Modern Real Estate Practice in Texas.* Dearborn Real Estate.

Nazmiye Balta-Ozkana, B. B. (2014). European smart home market development: Public views on technical and economic aspects across the United Kingdom, Germany and Italy. *Energy Research & Social Science*, 65-77.

NYDFS. (2015). *“Report on Cyber Security in the Insurance Sector”.* New York State Department of Financial Services.

NYDFS. (2017). CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES . *New York State Department of Financial Services*.

Parks Associates. (n.d.). *“European Smart Home Market Awakens”.* 2017.

Raiyn. (2014). *“A survey of Cyber Attack Detection Strategies”.*

Rawson, Duncan, & Jones. (2013). “The Truth About Customer Experience” . *Harvard Business Review*.

Robb, D. (2016). *Top Ten Big Data Storage Tools. .* InfoSTor.

RSA Insurance Group. (2018, April 7). *RSA Insurance Group History.* Retrieved from https://web.archive.org/web/20110902071509/http://www.rsagroup.com/rsa/pages/about us/history

Solomon. (2017). “Customer Service and the Insurance Industry: Best Practices We All Can Learn From”. *Forbes*.

Soltani, B. a. (2014). “Tiny Constables and the Cost of Surveillance”.

Statista. (2017). *Statista Digital Market Outlook - Smart Home Report 2017.*

US Bureau of Labour Statistics. (2018). *Occupational Outlook Handbook.*

USAA. (2018, March). Retrieved from USAA Corporate Website: https://www.usaa.com/inet/wc/home_security_main?akredirect=true

Varian. (2014). “Beyond Big Data”. *University of California Berkeley*.

White, M. D. (1998). How Benjamin Franklin became the "Father of the American Insurance". *Bank Insurance Marketing*.

Wiener Städtische. (2018, March). *EnergieBonus -.* Retrieved from www.wienerstaedtische.at: https://www.wienerstaedtische.at/fileadmin/user_upload/Dokumentenpool/Privat/Wohnen/Flyer_Energiebonus_26PG006.pdf

Wiening, E., Rejda, G., Luthardt, C., & Ferguson, C. (2002). *Personal Insurance (1st ed.).* Malvern, Pennsylvania.

Zion Market Research. (2016). “Smart Home Market: Global Industry Perspective, Comprehensive Analysis and Forecast, 2016-2022”.

Zurich UK. (2018, February). *Zurich announces partnership with Cocoon.* Retrieved from https://www.zurich.co.uk/en/about-us/media-centre/general-insurance-news/2016/zurich-announces-partnership-with-cocoon