Dear members and friends,

We have an interesting paper ("opinion") from EIOPA, considering the withdrawal of the UK from the EU.

The European Insurance and Occupational Pensions Authority (EIOPA) has issued an Opinion on the solvency position of insurers in light of the withdrawal of the United Kingdom (UK) from the European Union (EU).

The objective of this Opinion is to call upon national supervisory authorities to ensure that all risks to the solvency position of insurers arising from the UK becoming a third country are properly addressed.

National supervisory authorities should ensure that the insurance and reinsurance undertakings under their supervision identify, measure, monitor, manage and report the risks arising from the UK becoming a third country and include them in their own risk and solvency assessment.

Furthermore, national supervisory authorities should assess the risks affecting their national markets and, where necessary, take preventive supervisory actions.

The withdrawal of the UK from the EU might have an impact on the solvency position of insurers. Technical provisions, own funds and capital requirements of insurance and reinsurance undertakings in Member States other than the UK can change when the UK becomes a third country due to changed regulatory requirements.

In particular, Solvency II and other financial regulation distinguish between activities in and outside of the EU. The Opinion sets out 14 areas where the determination of the solvency position of insurers will change.
The areas include the risk-mitigating impact of derivatives, the recognition of ratings from UK rating agencies and the regulatory treatment of credit risk exposures situated in the UK.

Not all of the changes may affect each insurance company.

Together with national supervisory authorities, EIOPA will monitor the risks to the solvency position of insurance and reinsurance undertakings.

The monitoring will be proportionate to the nature, scale and complexity of the risks.

National supervisory authorities should provide to EIOPA the necessary information for this monitoring within the current European framework for supervisory cooperation.

Gabriel Bernardino, Chairman of EIOPA, said: “In their risk management, insurers should in particular prepare for the scenario that the UK becomes a third country and leaves the internal market. It is important that national supervisory authorities monitor and assess the risks to their national markets and take timely and effective supervisory actions.”

EIOPA defines its supervisory convergence priorities

- The supervisory convergence plan focuses on the implementation of Solvency II and conduct of business supervision.
- EIOPA defined three priority areas, namely the implementation of the common supervisory culture, addressing the risks to the internal market and to the level playing field which may lead to supervisory arbitrage as well as the supervision of emerging risks.

The European Insurance and Occupational Pensions Authority (EIOPA) published its supervisory convergence plan for 2018-2019 for the insurance sector, focusing on the implementation of Solvency II and conduct of business supervision.

Supervisory convergence should ensure a high, effective and consistent level of supervision throughout the European Union, granting a similar level of protection to all European policyholders and beneficiaries.

To strengthen further supervisory convergence for 2018 and 2019, EIOPA defined the following three priority areas:

1. Implementation of the common supervisory culture and new supervisory tools.
2. Risks to the internal market and the level playing field which may lead to supervisory arbitrage.

The implementation of a common supervisory culture will include the further specification of each of the key characteristics of the common supervisory culture.

In addition, EIOPA will develop common benchmarks for the supervision of internal models, work on a common basis for the supervisory assessment of conduct risks throughout a product’s life cycle, perform a thematic review on travel insurance and define good practices for the supervision of intra-group transactions and risks concentrations.
To address risks to the internal market and to the level playing field, EIOPA will analyse the consistency of the calculations of technical provisions in general and in a cross-border context in particular for non-life business such as the “decennial liability insurance” and “medical malpractice insurance”.

Furthermore, special attention will be paid to the assessment of internal model outcomes, the detection of potential unsustainable cross-border business models and the establishment of specific collaboration platforms where needed.

In the area of supervision of emerging risks, EIOPA will develop good practices on the supervision of IT security and governance, including supervisory expectations on insurance undertakings’ practices on cyber security and explore efficient ways to perform a cyber-attack penetration test.

A thematic review of the insurance industry’s use of big data as well as the monitoring of the potential consequences of the withdrawal of the United Kingdom from the European Union will continue to ensure consistency in supervisory approaches.

The priorities of the supervisory plan were identified according to their impact on policyholders and on financial stability as well as on the level playing field or the functioning of the internal market.

The priority areas include also those areas of supervision where practices across the European Union still differ substantially.

At the beginning of 2019, the supervisory convergence plan will be updated and include a progress report.

On conduct of business supervision, EIOPA has developed a broader strategy to address supervisory convergence from the conduct perspective.

The strategy underlines tools for improving market monitoring and risk identification and mitigation as well as developing proactive supervisory capacities across the European Union with the aim to tackle better potential consumer detriment.

Gabriel Bernardino, Chairman of EIOPA, said: “Achieving supervisory convergence, one of EIOPA’s strategic goals, requires a collective effort by all national supervisory authorities and EIOPA. This supervisory convergence plan sets key priority areas, which are crucial for achieving
high-quality and effective supervision and the implementation of a common supervisory culture across the European Union in the interest of the policy holders.”
The European Supervisory Authorities EBA, EIOPA, and ESMA (ESAs) conclude a multilateral Memorandum of Understanding with the EFTA Surveillance Authority

The European Supervisory Authorities (EBA, EIOPA, and ESMA - the ESAs) have concluded a multilateral Memorandum of Understanding (MoU) on cooperation, information exchange and consultation with the EFTA Surveillance Authority.

This multilateral MoU establishes practical arrangements between the ESAs and the EFTA Surveillance Authority in relation to the adoption of acts by the EFTA Surveillance Authority on product intervention, breach of European Economic Area law, action in emergency situations, mediation, as well as on the adoption of specific opinions, effective within the EEA-EFTA States.

The EFTA Surveillance Authority has been vested with the powers to adopt decisions and formal opinions addressed to competent authorities and/or financial market participants and financial institutions in the EEA-EFTA States based on the amended Agreement on the European Economic Area (EEA Agreement) of 30 September 2016.

The EEA Agreement guarantees equal rights and obligations within the Internal Market for individuals and economic operators in the European Economic Area.

It provides for the inclusion of European Union legislation covering the four freedoms — the free movement of goods, services, persons and capital — throughout the 31 European Economic Area States.

EFTA Surveillance Authority monitors compliance with the EEA Agreement in Iceland, Liechtenstein and Norway, enabling those Member States to participate in the Internal Market of the European Union.

It was established by the EEA Agreement, an international agreement which enables the three EFTA States to participate fully in the European internal (or single) market.
The EFTA Surveillance Authority’s role in the EEA-EFTA States mirrors the role of the ESAs in the European Union Member States.

To read it:
Iran and India ban cryptocurrencies

Iran’s central bank has banned Iranian banks, credit institutions and currency exchanges from selling or purchasing digital currencies. It says cryptocurrencies, like Bitcoin, are used in money-laundering and financing terrorism, and that they are inherently unreliable and risky.

The same concerns are expressed widely around the world, including by the Chief of the International Monetary Fund, but many also believe digital currencies and the technology behind them could have a positive effect as a low-cost payment method.

Iran’s actions follow similar decisions by other central banks, such as the Reserve Bank of India’s decision in April to serve three months’ notice for entities they regulate to cease dealing in digital currencies.

The central bank decisions have been concerning for digital currency users in these countries (reportedly around five million in India), but it is too early to say whether these actions will last, have any long-term impact on the wider cryptocurrency market or whether other countries will follow suit.

Some countries are debating the regulation of digital currencies: Japan has recently created a regulatory body for its cryptocurrency exchanges, for example, and others have considered creating their own state-backed digital currencies.

The future of digital currencies is still unknown, which is a major contributing factor to their price volatility, but they are likely to be with us for the foreseeable future.
How can Pan-European Personal Pensions (PEPP) work best for the European citizens?

Pan-European Pension Forum

Prague, 17 May 2018

Fausto Parente
Executive Director
European Insurance and Occupational Pensions Authority (EIOPA)
Current and Future Challenges of the Pensions Sector

The need to save (more) for future retirement income.

- **Demographic and employment trends**
  - Ageing population - People living longer
  - Unemployment - “broken careers”
  - “Unconventional” career paths and self-employment
  - Increasingly mobile workforce

- **Divergent pension landscape in Europe**
  - Challenged national budgets and state pensions
  - Stressed economic environment - low yields and negative interest rates
  - Low consumer trust - often low available income
  - Gender gap

To read the presentation:
The fintech phenomenon - five emerging habits that may influence effective fintech regulation
Opening remarks by Mr François Groepe, Deputy Governor of the South African Reserve Bank, at the Inaugural Intergovernmental Fintech Outreach Workshop, Council for Scientific and Industrial Research, Pretoria.

Introduction

Good morning, ladies and gentlemen.

Welcome to the inaugural Intergovernmental Fintech Outreach Workshop.

Let us begin with the words of Joseph Schumpeter: “Situations emerge in the process of creative destruction in which many firms may have to perish that nevertheless would be able to live on vigorously and usefully if they could weather a particular storm.”

There is no doubt that we are witnessing a wave of disruptive innovation and technology that one can liken to Schumpeter’s ‘creative destruction’, one that will leave no aspect of human endeavour untouched.

Financial services in particular are within the eye of the storm of the change as a result of financial technology, or ‘fintech’.

An elementary Google search on fintech results in no fewer than 35.2 million hits.

Investment in fintech over the last three years is estimated to have been well over US$300 billion dollars. Attention to the emergence of fintech has come from every quarter.

There have been contributions from the World Economic Forum reflecting the potential of distributed ledger technology across wide-ranging financial services and activities.

The International Monetary Fund has been vocal about the potential impact of cryptocurrencies. More recently, under the Argentinian
presidency, the G20 has committed to deepening the analysis on how financial inclusion could be achieved through digital innovations.

All of these examples suggest a heightened expectation of shifts to financial services as a result of fintech.

At the outset, it may be appropriate to attempt to define what fintech is.

‘Fintech’ usually refers to innovative start-ups or underlying technologies such as blockchain, cloud computing, and machine learning.

Founded on an activity-based analysis conducted by the Financial Stability Board (FSB), the evolving definition of ‘fintech’ is that it is neither the fintech firms, nor the start-ups, nor the emerging technologies.

Rather, ‘fintech’ is the technology-enabled innovation in financial services as a result of the process of ‘creative destruction’. It may lead to new business models and new configurations within financial services

To read more: https://www.bis.org/review/r180426e.pdf
Introductory statement - IIF International Capital Markets and Emerging Markets Roundtable
Dr Andreas Dombret, Member of the Executive Board of the Deutsche Bundesbank, at the IIF International Capital Markets and Emerging Markets Roundtable, Washington DC.

Ladies and gentlemen,

Ever since the ground-breaking work of Solow in the fifties most policy makers and members of academia - especially in the advanced economies - have inclined to favour free capital flows.

Many crises later, the view has somewhat shifted, in particular, regarding emerging markets and developing countries, which is the group of countries that I will focus my remarks on.

Not only can capital flow reversals and in the extreme form sudden stops create significant costs in terms of output losses, financial instability and even political instability. But from all we know today it is surprisingly difficult to find empirical evidence of capital account liberalization being beneficial in terms of output gains, investment, productivity gains, or risk sharing for countries that have not progressed sufficiently far in their institutional development.

Much of the work on this has been carried out by the IMF and indeed by Maurice Obstfeld himself, so Maurice should correct me if I am wrong, but essentially liberalized capital flows should go hand in hand with functioning judicial systems including well enforced property rights, developed and well regulated financial systems as well as stability-oriented macroeconomic policies. There are even longer lists, but these seem to be the minimum requirements.

So, given that these conditions are not always met fully, should countries resort to capital flow measures if faced with volatile flows?
By the way, I am using the IMF terminology of capital flow measures. These are basically capital controls plus those macroprudential measures that aim to limit financial stability risks arising from cross-border capital flows.

I think we all agree that sound domestic policies should always be the first line of defence and that capital flow measures should not substitute for warranted macroeconomic or exchange rate adjustments.

But it is also useful to state an obvious but often overlooked fact: Unlike restrictions on the current account, the imposition of capital flow measures is not under the jurisdiction of the IMF, thus, any country can basically adopt such controls as it deems necessary to regulate capital movements. However, capital flow policies are part of the Funds surveillance and as such open to an assessment of their impact on the International Monetary System.

Objectives of capital flow measures usually are to maintain monetary independence, to mitigate exchange rate pressures and to safeguard financial stability. However, capital controls also come with a cost, like impairments of financial markets and possible reductions of economic growth due to their distortions.

Evidence on the effectiveness of capital flow measures is mixed, or in the words of Olivier Blanchard: "still surprisingly inconclusive". Work on macroprudential measures has only begun in earnest after 2009, thus, the knowledge about these policies is still limited.

Significant results have been found on the composition of capital flows. There is evidence that they can lower banking inflows and portfolio inflows. But there is no significant evidence for a clear impact on net or gross flows. While there is solid evidence that capital flow measures help countries to conduct an independent monetary policy, there seems to be little or no effect of capital flow measures on the exchange rate.

Although the literature on the impact on financial stability is relatively young, capital flow measures have been found to lower credit growth and to curb bank leverage.

Where does that leave policy makers? There is still a lot we do not know. It seems capital flow measures can help a country to deal with volatile capital flows and reduce the likelihood of a financial crisis. But of course one has to consider the costs and distortions.
I think the Institutional View of the IMF has got it mostly right. To safeguard financial stability countries should be able to use all tools at their disposal, depending on which are best suited to the task, but as non-distortionary as possible and not as an excuse to shirk difficult decisions on macroeconomic policy.

Given that capital movements are not comparable to trade in real goods and given the diversity of its membership, I see no value in extending the IMF’s mandate beyond the existing arrangements regarding capital flows. This would necessitate also a change of the IMF’s Articles of Agreement, which could be opening a can of worms.
Ladies and Gentlemen,

I am very pleased to welcome you this morning to this presentation of the 2018 Financial Stability Review (RSF), dedicated to non-bank finance.

Intended as a forum for dialogue and exchange, the FSR offers leading personalities from diverse backgrounds the chance to have an open debate.

I am delighted to see many of this year's contributors here among us this morning, and I would like to extend my warm thanks to all the speakers: Klaas Knot, President of the Dutch Central Bank; Philip Lane, Governor of the Central Bank of Ireland; Robert Ophèle, President of the Autorité des marchés financiers; Paul Hamill, Global Head of FICC at Citadel Securities; Yves Perrier, CEO of Amundi; and Richard Portes, Professor of Economics at the London Business School.

The topic we have chosen to address is far from anodyne: according to the Financial Stability Board (FSB), non-bank financing totalled USD 160 trillion in 2016 [Monitoring Universe of Non-Bank Financial Intermediation, MUNFI], up 50% relative to 2008 and accounting for close to half of all financial assets held by financial institutions worldwide, compared with 40% in 2008.

And yet - or maybe precisely because of this - there is still much heated debate over its scope and over what exactly it should be called.

In order to better understand it, we need to rid ourselves of two mindsets: first, one of irrational fear, as non-bank finance also enables the financing of growth and innovation; and, in contrast, an over-idealised or "angelic"
vision of the sector, as shadow banking does indeed carry risks and regulators have a role to play in mitigating them.

1. Overcoming our irrational fears: the benefits of market-based financing

To overcome our irrational fears of non-bank finance, the words we use to describe it matter. Is it "shadow banking", with all the negative connotations this implies, or rather, as some regard it, "market-based finance" or "non-bank credit intermediation"?

For the title of this FSR, we have chosen the term "non-bank finance" in its broadest sense.

The work carried out by the FSB enables us to better determine its scope: the higher measure, which is entity-based [Other Financial Intermediaries or OFIs], puts the total at USD 99 trillion. However, those activities liable to pose a risk to financial stability, that is "narrow shadow banking", only account for USD 45 trillion, in other words a little under 30% of total non-bank finance.

Market-based finance is still not very widespread in the euro area: it accounts for just 20% of total non-financial corporation debt, with the remaining 80% taking the form of bank lending.

In the United States, these proportions are reversed. We should stress here that, of the larger euro area countries, France has the highest proportion of market-based financing, at 40%. Non-bank financing in France totals EUR 1.748 trillion, and the leading asset manager in Europe is a French firm, Amundi.

France also has an internationally recognised regulator, in the form of the AMF, while Paris is home to the European Securities and Markets Authority, ESMA. After Brexit, I also have every reason to believe that a significant share of the market activities of the largest global banks will be based in Paris.

First of all, I want to put an end to the non-debate over whether market-based finance is better than bank-based finance and vice versa, and the misconception that the US system should be replicated in Europe: working towards a balanced development of non-bank finance simply means giving companies the option of diversifying their debt financing. Fundamentally, the real debate lies elsewhere: it is about switching from debt to equity.
This is crucial in advanced economies, where growth is dependent on innovation. Equity financing is better suited to the uncertainty and often long-term returns associated with innovative projects.

The euro area is seriously lagging behind in this respect: equity only accounts for 74% of GDP, compared with 125% in the United States. Moreover, it only makes up half of the total external financing of euro area corporations (equity + debt), compared with three quarters in the United States.

In practice, how can we successfully diversify the sources of financing? At the national level, I am pleased to see that the "Pacte" law drafted by the Minister for the Economy and Finance seeks to foster long-term and equity-based life insurance contracts - by overhauling Eurocroissance - and encourage and simplify retirement savings, including the annuity component which has the longest investment horizon.

Moreover, one approach supported by the Banque de France is the implementation of an ambitious European framework: a "Financing Union for Investment and Innovation" to better channel the euro area's EUR 400 billion savings surplus into equity financing and innovation.

This Financing Union needs to unite and build on existing initiatives, first and foremost the Capital Markets Union, but also the Banking Union and the Juncker Investment Plan. It also means making concrete progress in several areas: the revision of accounting rules, taxation and insolvency laws in order to facilitate cross-border investment, notably in equity; the European-wide development of long-term savings products and investment vehicles such as venture capital funds; the completion of the Banking Union.

2. Avoiding an angelic vision: monitoring, testing, regulating

So no irrational fears in the face of the shadows; but no angelic vision either. A portion of shadow banking is still overly exposed to credit, liquidity, leverage and maturity risk, and there is significant potential for these to spread to the rest of the financial system and cause financial instability. We discussed this issue at the IMF and G20 meetings in Washington just last week.

In my view, therefore, there are three priorities for regulators: monitoring, testing and regulating.
Monitoring first, thanks to the compilation of detailed data on shadow banking.

The FSB already contributes to this with its annual report on shadow banking, as does the ESRB with its European Union shadow banking monitor.

But we need to go further: we need an even more precise picture of the sector as participants and business models can vary considerably from one country to another, and are sometimes extremely complex. It is particularly crucial to put together a mapping of the interconnections within the shadow banking sector and with traditional banks and insurers.

The second priority is to be able to test for systemic risks, using appropriate tools.

In order to measure the global impact of shocks, we have a particular need for liquidity macro stress-tests that take into account investment funds: the latter are especially vulnerable to runs, in the event of a stock market crash for example, if they are open-ended and have no system of gates.

To achieve this, we need to develop, jointly and at a global level, a harmonised framework for systemic stress tests: the FSB already recommended such tools in 2017, but there is a real risk that they will remain in the exploratory phase, and that no action will be taken at the level of the financial system.

The third and last priority is to regulate. Following the finalisation of the Basel III reform in December 2017, the main focus for financial regulation is no longer bank solvency, but non-bank liquidity.

We nonetheless need to avoid making two mistakes.

The first would be to favour one sector over another, be it banks or shadow banking: the existence of opportunities for regulatory arbitrage could to lead to the transfer of capital-intensive activities to less regulated, or even unregulated entities, which would be counterproductive.

The other mistake would be to impose banking regulation on shadow banking, as the risks are not the same; in particular, the same capital requirements cannot be applied.

At the global level, the non-bank sector needs to be provided with microprudential and macroprudential regulations that are tailored to its particular business model and risks.
With regard to macroprudential regulation, France is a pioneer in this field with its decision to introduce, as of 1 July this year, a measure regarding large enterprises that also takes into account their market debt. We shall publish details on how it will work this week.

But we need to be honest with ourselves and admit that our experience of using macroprudential tools outside the bank sector is still very limited.

One of our priorities in terms of regulation should also be to develop liquidity management tools for investment funds, and to refine the measurement of their leverage, two issues that, fortunately, the FSB has already identified.

It is also important that we increase the transparency of shadow banking activities.

In this respect, the entry into force of the European regulations EMIR2 and SFTR should be a considerable step forward.

As I've been talking about macroprudential measures regarding large corporations, and our subject is financial stability, I'd like to bring you up to date on bank lending in France: lending to the private sector - to households and businesses - is growing rapidly in France, at a rate of close to 6% per year. At the next meeting of the High Council for Financial Stability (HCSF) in June, we shall look at whether we need to introduce additional measures.

To sum up, we have not yet finished exploring the issue of non-bank finance and I am certain that today's event will make a valuable contribution to the debate. I would like to pass the floor now to Aurélia End, who will host the round table, and wish you all an excellent morning.
Symantec have reported that a group they have tracked as ‘Orangeworm’ since 2015 are targeting the healthcare industry in the United States, Asia and Europe, including the UK.

40% of their attacks focus on the healthcare industry.

Other industries targeted are either closely related to healthcare or part of the supply chain, including IT, manufacturing, logistics and agriculture.

It is likely that the supply chain has been deliberately targeted to gain access to their customers’ environments.

After gaining access to the target environment the group deploy a custom malware trojan, allowing attackers to remotely access the compromised device.

The malware collects information about the computer to determine if it may be of interest, before "aggressively" copying itself to other systems with open network shares.

The trojan uses an older propagation method that mainly works on older operating systems, and the health sector is known to use legacy systems on older platforms.

It has been discovered on devices hosting software used for high-tech imaging devices such as MRI and X-rays, as well as devices used to complete consent forms.

The group’s exact motives are unclear. However, it is likely that they are interested in obtaining personal or proprietary information, possibly for identity theft, extortion or corporate espionage.

In the UK, the Department of Health and Social Care recently announced a funding package to improve their cyber security capabilities. The package of measures includes ensuring that all UK health and care organisations are using the latest Windows 10 software with up-to-date security settings.
The implementation of this upgrade and other basic hygiene measures should prevent malware, like the Kwampirs trojan, from exploiting NHS legacy vulnerabilities.
STRENGTHENING NETWORK & INFORMATION SECURITY, PROTECTING AGAINST ONLINE DISINFORMATION ("FAKE NEWS")

For the purpose of this paper, “online disinformation” is defined as: “false, inaccurate, or misleading online information designed, presented and promoted with malicious intent or for profit”.

“Fake news” has recently received a lot of media attention as a potential disruptor of democratic processes globally. There is a need to initiate a dialogue in the EU around the possible responses to this phenomenon.

In this regard, the misuse of:

• a computer connected to the internet,
• a compromised online account,
• a fake online account, or
• online platforms

may be characterised as a weapon, where posting on social media, emails, spam and other online activities can cause damage to others, as well as to society at large.

Recent events suggest that the dissemination of online disinformation is posing an increasing threat to the effective functioning of the democratic process.

This trend is exemplified by the 2016 U.S. presidential elections where, in a December 2016 survey, 64% of U.S. respondents held that fake news caused a great deal of confusion about the basic facts of contemporary events.

Subsequent allegations of cyber meddling in elections in the EU context reported in the media include the French presidential elections and the British EU membership referendum.

A key factor in the dissemination of online disinformation is human behaviour. According to research findings, false claims are shared more
than true ones, and false stories gain more attention and are disseminated at a higher speed.

Equally important is the amplifier phenomenon, which concerns accounts that disseminate large amounts of false information aimed at manipulating public opinion.

In this paper, ENISA presents some views on the problem of online disinformation in the EU from a Network and Information Security (NIS) perspective.

A number of recommendations are presented, which relate both to general NIS measures, as well as targeted measures to protect against online disinformation specifically.

This opinion paper was presented as input to the European Commission’s Communication “Tackling Online Disinformation: A European Approach”, which was published in April 2018.

To read more: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/fake-news
The Value of Personal Online Data

Introduction

Data is considered to be the gold of the digital age.

A gold rush is ongoing within businesses operating in highly competitive markets looking for data and information about all aspects of human life such as consumer behaviour, social and political orientation, money spending habits, health, lifestyle, etc.

Data has become an important commodity generating profits on its own; and data collection has become the main activity for numerus businesses.

The estimated ARPU (average revenue per user) in digital advertisement, mainly controlled by Google and Facebook, reached $59 per person in 2017.

Multiplying this number by an average 3.8 billion internet active users, we can roughly estimate the size of this business.

The collection and analysis of personal data is not only important for businesses but for society in general: policy decisions taken based on personal data analysis and medical research using patients and caregivers data to improve healthcare are just few examples.

While the benefits from collecting and analysing personal data are evident for a large number of actors/organisation, various interests recurrently challenge its protection.

This cybersecurity info note reviews recent challenges in data protection and the impact to our society on the occasion of the abuse of 87 million Facebook profiles for the purpose of US election campaigns through Cambridge Analytica.

Though this incident is at initial stages of analysis, there are grounds to believe that it is the top of the iceberg with regard to available practices in harvesting user data, analysing and acting upon the results for a variety of objectives.
Contextual Information

The recent Facebook and Cambridge Analytica incident confirmed what was already known, at least within data privacy experts: online digital services use personal data to monetize their business models and politicians leverage from big data analytics to support election campaigns.

At a first glance, it has become public – revealed by a whistle-blower - that Facebook deliberately opened a door in 2013 for a third-party app to harvest personal data without the user’s consent.

Cambridge Analytica - a British political consulting firm – obtained access to a database with personal data from 87 million Facebook accounts (initially estimated in 50 million) collected via a third-party app offering a free personality test quiz.

The owner of the app, Aleksandr Kogan a Cambridge University Psychology Professor, took advantage of a Facebook privacy breach and legally obtained consent from 200,000 users to access their personal data, including details about their friends who in any case were not in a position to provide their consent.

This way, the app owner increased the number of Facebook accounts accessed and the amount of personal data harvested by ca. 250 times. Moreover, according to the whistle-blower, a database with the harvested data was later shared with Cambridge Analytica, utilized for political analysis and Facebook advertisement in support of political campaigns.

In the attempt to apologise for the incident, Facebook CEO could not confirm which other third-party apps took advantage of this privacy breach between 2013 and 2015, and if other copies of the data possessed by Cambridge Analytic were distributed.

Furthermore, Facebook recently acknowledged a breach in its search engine and account recovery functions that it said could have exposed “most” of its 2 billion users to having their public profile information harvested.

Investigations over Facebook conduct and practices with regards of processing personal data (PII) and free movement of such data are not new.

In the past the Canadian Privacy Regulator, US Federal Trade Commission and EU Data Protection Authorities from UK, Ireland, Belgium, Norway
and Germany scrutinized the practices of the social media giant imposing significant changes to its software. The European Union data protection acts, 1988 and 2003 - EU Data Protection Directive 95/46/EC - adopted in 1995 introduced important legislation into EU Member States legal systems, allowing the investigation of such incidents and consequent legal prosecution.

The General Data Protection Regulation (GDPR), due to come in force May 2018 superseding this directive, will have significant impact on companies such as Google, Facebook and Twitter who if proven, could face huge fines for this type of incidents.

Nonetheless, in the realm of this incident, there are some further investigations regarding various data collection activities that have been performed by Facebook in the past; and some debates are coming up regarding the consistency/coverage of privacy issues mentioned in user agreements.

Furthermore, a news media investigation uncovered the actions of Cambridge Analytica that included the use of personal data analytics to format political messages published in the social media in an attempt to manipulate the public opinion towards specific electoral candidates.

This revelation occurs while the civil society still debates and the judiciary investigates alleged foreign interference in the 2016 US presidential elections and UK Brexit referendum using social media adds and fake news.

This incident also demonstrated the power of big data analysis: service offerings go beyond traditional statistics and may support any objective related to human behaviour, such as supporting of election campaigns.

Cambridge Analytica publicly announced how their services influenced elections around the world.

Though formally lawful, such interventions may move usage of user data in grey zones.

The incident has made clear that a lot of discussion is still pending about data privacy issues and about potential regulation needs in the usage of big data.

Such regulation come to complement data protection regulation to cover appropriateness and legitimation of data analysis campaigns.
Recommendations

Users are advised to reevaluate their privacy settings in the digital world by taking the following actions:

- Avoid subscribing or installing suspicious third-party apps - Those are common on the network and most request access to personal data without the user noticing.

- Review which services or apps are sharing personal data – Digital platforms offer third-party authentication services to other applications. Users are advised to review which applications and services are connected to their accounts.

- Change privacy settings – Digital platforms have many privacy settings available to control who can have access to personal information.

- Review the privacy policy before subscribing to digital applications and services – Policies are long and hard to read but these are meant to inform users about their commitment to privacy protection.

Closing Remarks

People’s confidence in digital players to protect their privacy has been recurrently undermined by these type of incidents, with serious impact in credibility and trust in the digital economy.

We cannot expect that data carers will proactively revert this situation by regulating themselves putting an end to a situation that ultimately generates large profits for them. Since the start of this incident, Facebook already lost US $80 billion in market value (ca. 18% depreciation in stock price) followed by other social media giants Google (ca. 7%) and Twitter (ca. 20%).

The way the story evolves, it is premature to anticipate what will be the result and predict what will be the outlook of companies and business models that rely exclusively in the monetization of personal data.
An annuity is a very serious business

Today I am going to talk about the bulk purchase annuity market, the increasing use by life insurers of illiquid assets – and in particular equity release mortgages – to back these annuities and the significance of the Solvency II matching adjustment.

First, though, I want to reflect briefly on the UK life insurance sector as a whole.

Standing here in 2018 it is a very different market to the one I might have been describing just 20 years ago.

The big change is that most new life and pension products do not guarantee returns.

The great majority of savings products are unit linked. And individual pensioners are increasingly choosing draw down products rather than annuities.

In both cases, investment risks lie with the policyholders.

Other things being equal, that should mean a less risky life insurance sector and fewer sleepless nights for a prudential supervisor like me.

The other side of the current life insurance market though is managing the legacy of past promises.

Two trends are clear here: first, a very active market in transfers of books of annuities and closed life books between firms, with insurers specialising in particular niches; second, transfers of annuities to life insurers from corporate, defined benefit pension schemes – the bulk purchase annuity market that is the subject of this conference.
Risks for insurers in the bulk purchase annuity market

The bulk purchase market has grown over recent years from a flow of around £5bn in 2010 to over £10bn in each of the past four years.

With the funding position of many defined benefit schemes improving and company boards still keen to shed pension risks, commentators expect the market to expand further. Transfers in excess of £15bn are predicted this year.

The number of life insurers active in this market has increased, with most of them seeing it as a priority for future growth.

Our sense is that the market has become more competitive. This is good news for UK companies seeking to shed pension risks.

For the insurers, finer margins make it more important that they understand the risks on deals and get the pricing right.

A concern is that firms might relax risk management standards or take short cuts in order to win deals and meet new business targets.

I want to highlight three areas of risk: data due diligence; longevity and its reinsurance; and asset selection, rating and valuation.

I will touch briefly on the first two before spending more time on the third.

On data due diligence, it seems obvious to say that insurers should not enter into bulk purchase transactions without understanding in some depth the nature of the annuity liabilities they are taking on.

But this is an area where we see firms taking different approaches and willing to price with different levels of risks.

One particular aspect is whether insurers have a full picture of their potential obligations to pensioner spouses and dependents.

Insurers need to be clear about their appetite in relation to data risks. Most of the longevity risk on new transactions is currently being reinsured, often outside of the UK.

To read more:
https://www.bis.org/review/r180511d.pdf
Joint EU-U.S. statement following the EU-U.S. Justice and Home Affairs Ministerial Meeting

On 22 and 23 May 2018, the EU-U.S. Ministerial Meeting on Justice and Home Affairs was hosted by the Bulgarian Presidency of the EU Council in Sofia, Bulgaria.

The meeting reaffirmed the long-standing, fruitful cooperation between the United States of America and the European Union in the areas of justice and home affairs, as well as the importance of jointly addressing common security threats.

The United States was represented by the U.S. Attorney General, Jeff Sessions, and the Acting Deputy Secretary for Homeland Security, Claire Grady.

The European Union, hosting the meeting, was represented by the Commissioner for Migration, Home Affairs and Citizenship Dimitris Avramopoulos, the Commissioner for Justice, Consumers and Gender Equality Věra Jourová, the Commissioner for the Security Union Julian King, as well as Bulgarian Minister of Interior Valentin Radev and Minister of Justice Tsetska Tsacheva, together with Austrian Federal Minister for the Interior Herbert Kickl and Federal Minister for Constitutional Affairs, Reforms, Deregulation and Justice Josef Moser, on behalf of the current and incoming Presidencies of the Council of the European Union.

The European Union and the United States discussed their shared efforts to combat terrorism, focusing on effective information sharing, preventing radicalization, use of the internet for terrorist purposes, and vigilance with respect to aviation security, and chemical, biological, radiological and nuclear threats, and explosives, especially in relation to the evolving chemical threats to aviation and in public spaces.

With regard to EU-U.S. information sharing on Passenger Name Records (PNR), participants of the meeting emphasized the importance of such sharing, and noted impending developments in the separate EU-Canada PNR discussions.

The participants agreed to continue the discussion of PNR, at the next EU-U.S. Ministerial, which will take place in Washington, D.C., in the second half of 2018.
Participants also discussed security and law enforcement cooperation in cyber-space, affirming the importance of allowing swift access to electronic evidence by law enforcement and judicial authorities, while also protecting privacy and civil liberties.

Similarly, they stressed the need to maintain a safe, open, and secure cyberspace for the promotion of economic and social development, and exchanged views on how to best address this growing challenge.

The European Union and the United States also exchanged information on developments in the area of migration, border management, and their respective visa policies.

The European Union provided an update on migration trends in Europe and ongoing initiatives to enhance the management of its external borders; the European Union and the United States took stock of the continuing progress by the European Union and the United States, including that of the five concerned EU Member States, towards meeting the statutory requirements of the Visa Waiver Program, in order to be considered for designation.

Both sides also acknowledged the need for strengthening operational cooperation to effectively prevent and eradicate migrant smuggling and trafficking in human beings, and also discussed the importance of secure and lawful immigration systems.

Finally, the United States and European Union discussed the importance of ensuring swift exchange of financial information and improving the effectiveness of financial investigations.

The European Union and the United States discussed the latest developments in these areas and shared best practices in an effort to step up their common fight against anti-money laundering and terrorism financing.

Underlining the progress made in these vital areas of common interest, and re-emphasizing the fact that common solutions are necessary in order to address global security threats, the European Union and the United States committed to meet again in the second half of 2018 in Washington, D.C.
Disclaimer

Despite the great care taken to prepare this newsletter, we cannot guarantee that all information is current or accurate. If errors are brought to our attention, we will try to correct them, and we will publish the correct information to the LinkedIn and Facebook pages of the association.

Readers will make their own determination of how suitable the information is for their usage and intent. The association expressly disclaims all warranties, either expressed or implied, including any implied warranty of fitness for a particular purpose, and neither assumes nor authorizes any other person to assume for it any liability in connection with the information or training programs provided.

The association and its employees will not be liable for any loss or damages of any nature, either direct or indirect, arising from use of the information provided on this newsletter, or our web sites.

We are not responsible for opinions and information posted by others on this website. The inclusion of links to other sites does not necessarily imply a recommendation or endorse the views expressed within them. Links from this site to other sites are presented as a convenience to users. The association does not accept any responsibility for the content, accuracy, reliability, or currency found on external sites.

This information:
- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;
- should not be relied on in the particular context of enforcement or similar regulatory action;
- is not necessarily comprehensive, complete, or up to date;
- is sometimes linked to external sites over which the association has no control and for which the association assumes no responsibility;
- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);
- is in no way constitutive of interpretative;
- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;
- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts. It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

Solvency ii Association
Solvency II Association

1. Membership - Become a standard, premium or lifetime member.

You may visit:
www.solvency-ii-association.com/How_to_become_member.htm

2. Monthly Updates - At the Reading Room of the association.

3. Training and Certification – Become a Certified Solvency ii Professional.

Distance learning and certification:
www.solvency-ii-association.com/CSiiP_Distance_Learning_Online_Certification_Program.htm

For instructor-led training, you may contact us.