IT'S GETTING PERSONAL

Banks and insurance companies provide services that we cannot do without. But we are not in day-to-day contact with our bank or insurance company. Banks and insurance companies want to change this before they are outcompeted by companies like Google and Facebook.

Artificial intelligence and sensor technology is driving the development of new business models in the financial sector. Access to data from, among other sources, social media, mobile apps, location data and sensors has prompted a race to acquire as much data as possible about customers, in order to predict their behaviour, desires and needs.

The changes in the finance and insurance industries will affect our privacy. How deep into our lives do we allow insurers? Who will have access to our banking data and how will it be used and re-used? How can we keep the consumer in control in a complex business environment?

WHY NOW?

Why are these major changes happening in the financial sector right now? Firstly, the trend is being driven by the fact that it is becoming easier to collect, store and analyse vast quantities of data, at rapidly plummeting costs. Increased expectations among consumers are also a driving force. Consumers have become used to quick and easy access to services on their smart phones. Ample availability and user-friendliness are crucial if consumers are to make use of new services.

Demographics constitute a third, related, driving force. The so-called digital natives, those who have grown up with a smart phone in their hands, have higher expectations with regard to what a service should deliver than previous

generations. Nor do they have the same sense of loyalty to traditional institutions, such as banks and insurance companies, and are more open to using services delivered by new players.

Fourthly, regulatory changes are encouraging innovation and new business models. In January 2018, the EU's Payment Services Directive 2 comes into force. This opens the markets for banking, finance and payment services to new players who, with our consent, can obtain direct access to our accounts and transactions. Banks will no longer have monopoly on our account information, and new services for managing our private finances will emerge. On 24 May 2018, today's data protection legislation will be replaced by a new EU regulation. The new General Data Protection Regulation (GDPR) will also create an overall framework for how personal data may be collected and used for the development of personalised insurance and banking services.

PAY AS YOU LIVE – NEW INSURANCE MODELS

Rema 1000, a major supermarket chain in Norway, has expanded into the insurance market. Customers who want to buy car insurance from the company are offered a lower price if they install a device that monitors the driver's behaviour behind the wheel. The device registers, among other things, how fast the vehicle goes, whether the driver accelerates fast and brakes hard, and whether the vehicle is driven at night. This data is sent to an app, which assesses the driver's level of proficiency.[1] Rema 1000 is the first Norwegian company to offer personalised car insurance to all its customers, but several other insurance companies have launched pilot projects.

New technology is the most important driver for new business models in the insurance industry. By means of sensors in our vehicles, homes and on our bodies, insurance companies can collect real-time data about how we live and behave. Our insurance premium will be calculated on the basis of our own unique patterns of behaviour and not, as today, on the basis of statistical knowledge of how people similar to us have behaved previously.

In exchange for allowing sensors into our lives we become eligible for cheaper insurance. As personalised insurance arrangements gradually take over the

[1] https://www.remaforsikring.no/forsikringer/bil/

market, it is not certain that “pay as you live” schemes will necessarily mean lower-cost insurance for everyone. The sensors you allow into your life could also reveal that you are living anything but a healthy, risk-free life. Your reckless driving, lack of regular exercise and habit of leaving the tumble dryer on overnight could, on the contrary, result in higher insurance premiums.

Use of sensor technology not only makes it possible to offer individualised insurance premiums, it also enables insurance companies to influence their customers’ lifestyles. Insurance companies can make substantial savings by encouraging and rewarding risk-reducing behaviour. Rema 1000 offers a 15 per cent discount to customers who drive safely. Generali Group, one of the world’s largest insurance companies, offers a so-called Vitality programme in Germany, Italy, France and Austria, among other countries. [2] Under the programme’s motto “A little healthier every day”, customers can achieve discounts on their health insurance and health-related products in exchange for sharing data about their level of activity and eating habits. According to Generali Group, the objective of the programme is to encourage the adoption of a healthier lifestyle.

Insurance companies want to establish a more central role in our lives. At present, they do not have a close, day-to-day dialogue with their customers. Unlike a supermarket chain with a loyalty card, insurance companies do not have detailed information about their customers that can be used to deduce their interests and desires. This changes when the insurance companies start using sensor technologies that can collect real-time data about people’s behaviour. In the longer term, insurance companies could potentially possess more data about how we live our lives, at home, at work, on holiday, as we travel here and there, than any other companies in the world. It is, in this context, interesting to note that Google has signed off on at least six separate partnerships and investments in insurance tech in 2015, according to a CB Insights analysis of its activity. [3]

[2] Christl, Wolfie and Sarah Spiekermann, “Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data and Privacy”, Facultas, Wien, 2016

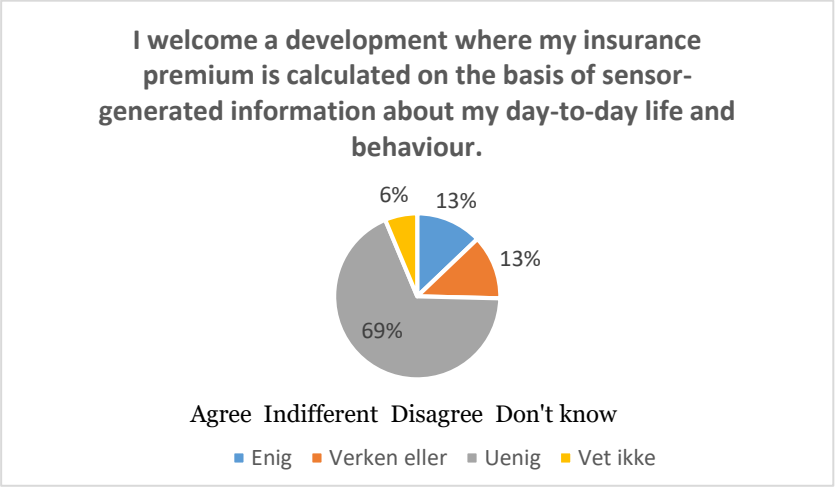
[3] Google’s Investments And Partnerships In Insurance Tech”
, 6.12.2016, https://www.cbinsights.com/blog/google-insurance-tech-investments/

New partnerships

In the USA, we are seeing a trend in which insurance companies are joining forces with suppliers of wearable technologies. Both the technology suppliers and the insurance companies benefit from this by reaching out to more customers. Fitbit, a market leader in health and fitness wristbands, has partnered with a number of US insurance companies. Vitality Group, an insurance company, rewards customers who use Apple Watch and who share data collected by the watch with the insurance company.[4] The company Beam Dental has developed a dental insurance policy in conjunction with the producer of a sensor-based toothbrush, which sends data about the user's dental health to the insurance company.

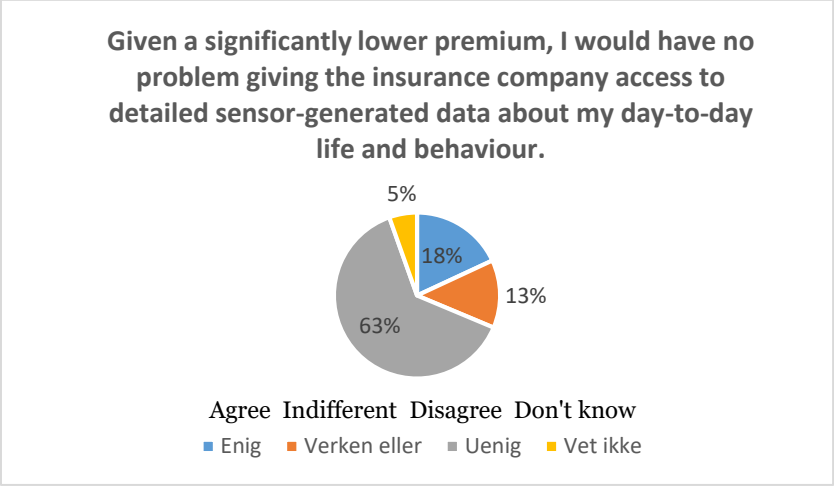
The majority do not want personalised insurance

The insurance industry is launching new, personalised insurance models. But do most people want these new models? In this year's privacy survey, we wanted to look into what people feel about personalised insurance schemes. The survey found that around 70 per cent of respondents do not want insurance premiums to be calculated on the basis of detailed sensor-generated data about their day-to-day lives and behaviour. Only 13 per cent of respondents were positive. However, it is worth noting that those over the age of 50 (63 per cent) were more negative than those under the age of 30 (32 per cent negative).



[4] Wearable technology: gathering data from tooth to toe, 21.11.2016, https://www.ft.com/content/9b00b05c-70fe-11e6-a0c9-1365ce54b926

If, however, insurance schemes based on our personal behaviours resulted in lower-cost insurance - would people be more positive? The majority of those asked (63 per cent) would not give an insurance company access to detailed sensor-generated data about their day-to-day lives and behaviours, even if it resulted in significantly lower insurance costs. Once again, those over the age of 50 were more sceptical about providing sensor data (56 per cent) than those under the age of 50 (31 per cent negative).



More open to share vehicle data than health data

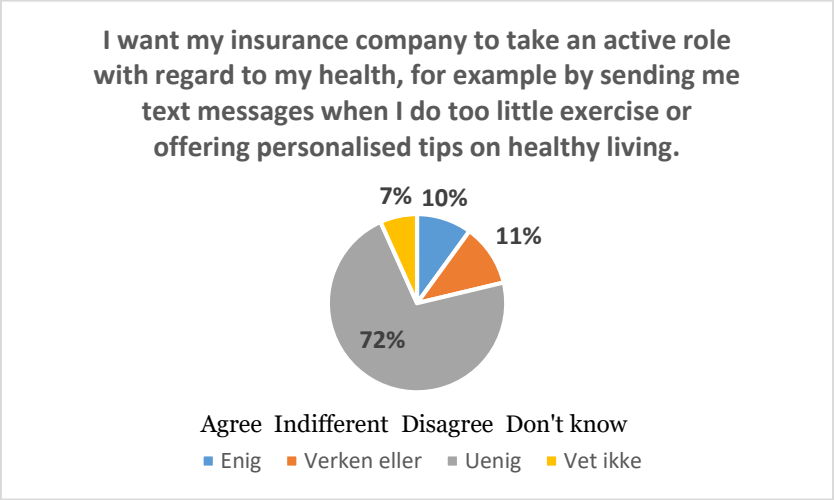
We also asked people whether they would like the price of car insurance to be based on data about how they actually drive. Around 40 per cent were negative, while roughly the same percentage were positive.

When it comes to life and health insurance, however, people are more sceptical about giving access to their data. Asked if they would like the price of life or disability insurance to be based on health-related, sensor-generated data, such as physical activity/exercise, pulse, calorie consumption and sleep, only 17 per cent of respondents said they were positive. 64 per cent were negative.

People are far more inclined to share health-related data with government authorities. As we shall see later in this report, a substantial 65 per cent would be willing to share information derived from fitness and health apps as a contribution to medical research.

Don’t want to be watched over by an insurance company

Insurance companies in Europe are trialling models in which they take an active role with regard to people’s health. But to what extent do people want insurance companies to involve themselves in personal health matters, for example by sending text messages reminding them to take some exercise or providing personalised health hints? 72 per cent were negative to such an idea, only 10 per cent responded positively. The figures indicate substantial scepticism about involving insurance companies in matters relating to one’s own health and level of physical activity. Here too, people are more positive about follow-up from the public authorities. 62 per cent want to be notified by the health service if their health or exercise information shows that they are at risk of developing a lifestyle illness.



Your online life determines the price

In November 2016, Admiral, one of the largest insurance companies in the UK, launched an insurance product in which customers could consent to the company analysing their Facebook account. In this way, drivers who had not been insured before could get cheaper car insurance. Admiral wanted to analyse customers’ behaviour on Facebook. Among other things, they wanted to see which words and expressions customers used in order to determine how conscientious and well-organised they were. However, immediately after the launch of this product, Facebook said that it would not permit user data to be applied in this way – even if its users gave their consent.

"EVERYTHING IS RELEVANT" - BIG DATA IN CREDIT RATINGS

Are you planning to buy a new car, rent an apartment or apply for a bank loan? The first thing that will happen is that your credit rating will be checked, so that the car dealer, landlord or bank can make sure you are able to pay for the service you are seeking. A negative credit rating can have major consequences for you. Transparency, verifiability and consistency with regard to how the credit rating is performed is therefore important.

In Norway, the credit rating business is regulated through licences issued by the Norwegian Data Protection Authority. This licence specifies, among other things, which data the credit rating agencies can use, for example information from the Norwegian National Registry, your annual tax return and payslips. Register data older than three years cannot be used as part of the assessment. Old sins should not be allowed to haunt you for the rest of your life.

Some credit rating agencies in Europe have started to rethink which data and data sources could be used to assess people's risk profile. Companies which make use of big data technology have emerged in recent years. They also assess individuals' credit ratings on the basis of their online activity, so-called behavioural data. By collecting and analysing behavioural data, these companies train algorithms that can predict whether you are a reliable payer or not. Your online footprint can reveal whether you are impulsive and featherbrained or responsible and dutiful.

German company Kreditech assesses the credit ratings of customers by means of machine learning algorithms that analyse more than 20,000 unique data points for each customer. Kreditech no longer publicly discloses which data sources it uses. Previously, however, the company's website stated that it based its analysis partly on which websites were visited, location data, contact lists, online purchase history and activity on social media. [5]

Almost all the companies that base their credit rating on behavioural data emphasise that they do so to help people who would otherwise not have access to banking services because information about them cannot be found in official registers.[6] Requiring people to agree to disclose their online history in order to obtain a loan, is, however, ethically dubious. There may be many reasons why

[5] Norwegian Data Protection Authority, "Big Data – Principle of privacy under pressure", 2013
[6] Christl, Wolfie and Sarah Spiekermann, "Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data and Privacy", Facultas, Wien, 2016

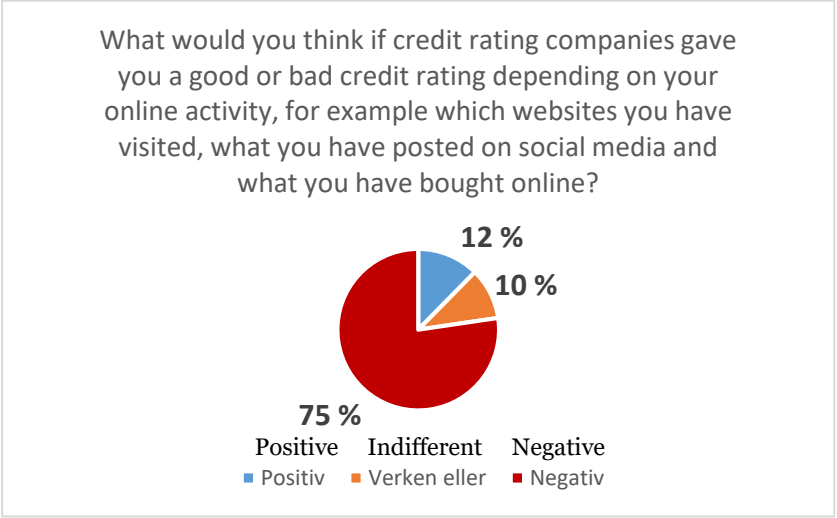
credit rating businesses choose to use behavioural data rather than data from public records. One of them may be that it is quicker, and therefore cheaper to calculate a credit score in this way.

Under current legislation, credit rating companies domiciled in Norway would not be permitted to use methods similar to those adopted by Kreditech. With the introduction of the new General Data Protection Regulation (GDPR) in 2018, today's licensing scheme will probably be abandoned. The question is therefore whether Norwegian credit rating agencies will be at greater liberty to use more sources of data than they are able to today.

The GDPR's requirements with respect to relevance and data minimisation, for example, will limit the types of data than may be processed. It will be up to each individual member state to enforce the requirements. Harmonising the requirements to which the sector is subject will be a challenge. The sector itself can play an important role by establishing industry-wide standards to secure equal terms and conditions.

People negative to credit rating based on on-line activity

Our survey shows that people are overwhelmingly negative to their online activity, i.e. which websites they visit or what they publish on social media, being used to assess their creditworthiness. 75 per cent are slightly or extremely negative to such a scenario.



China is developing a national credit rating system

Where you have been, what you buy, who you know, how many points you have on your driving licence, how your students rate you. These are just some of the factors the Chinese authorities wish to use to give all their citizens a credit rating. The system is called the Social Credit System (SCS), and its assessments are produced by combining personal data from banks, eCommerce and social media. In addition to performing a credit rating, the system can also be used by landlords, employers and potential sweethearts to assess what kind of person you are.

Sesame Credit is one of the first of the system's functions. It has been developed by Ant Financial, a subsidiary of Chinese eCommerce giant Alibaba. Sesame Credit is an assessment system that awards citizens points ranging between 350 and 950, depending partly on the individual's financial background. If you spend a lot of money via Alibaba's payment app Alipay, or you carry out financial transactions involving friends through Sesame Credit, your score will rise. The higher your score, the more opportunities open up. If you score more than 600 points, you can hire a car without paying a deposit. If you have more than 650 points, you can check out of hotels faster. And having more than 700 points makes it easier to get a visa to Singapore.

The objective of the SCS is to create a national system that collects data from many different sources, both public registers and commercial sources, such as social media, and it is intended to encompass all citizens. The system will be in place by 2020. Chinese authorities already have a website which allows anyone to check out other people's credit ratings. The website uses data from 37 key registers, and operates with the help of Baidu, China's largest search engine. [7]

[7] https://www.newscientist.com/article/dn28314-inside-chinas-plan-to-give-every-citizen-a-character-score/

FACEBOOK – YOUR NEXT BANK

«Banking is necessary, banks are not.»

Bill Gates

It is a long time since you had to visit a bank in order to pay your bills. In future, today's online banking systems will seem just as old-fashioned. The next generation of banks will be a personal assistant which, with the help of artificial intelligence, will perform services for you before you yourself even know you need them. They will keep track of your spending, tip you off about discounts on products they know you like, make sure you use the cheapest electricity supplier and move your savings where they generate the highest returns. The companies that have access to the most information about you, not just your income and spending, but also about your social network, day-to-day routines, interests and opinions, will be the best equipped to provide targeted and personalised financial services.

With the introduction of the revised Payment Services Directive in 2018, players like Google, Facebook and Amazon will be able to provide you with banking services. You will be able to grant players outside the banking sector access to your accounts and transaction information. Facebook has recently unveiled their newly acquired licenses for e-money and payment services out of Ireland.

Banks are positioning themselves to avoid being outcompeted by new enterprises. In Norway, DNB has considerable success with its app Vipps, a mobile payment application designed for smartphones. The app has over 2 million Norwegian users and is Norway's largest payment application.The real value in this type of service however, is not primarily in the transactional revenues it brings, but in the possibility the service provides for enhanced customer insights. Vipps is a social network that provides DNB with valuable data about its users, for example about their social circle, their movement pattern and where they shop. This is data the bank can use for marketing purposes and to develop new services.

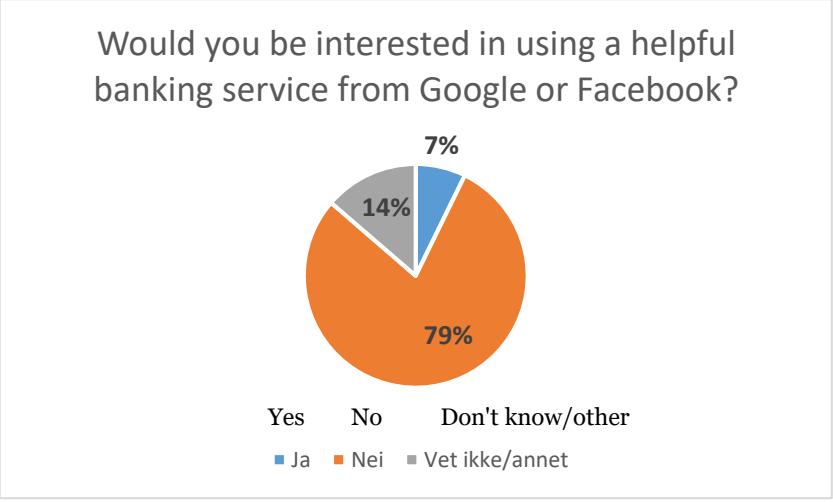
All the major banks in Norway have also established programmes in which they invite fintech start-ups to develop new digital services based on their banking data. The government is also on the ball, and has announced plans to establish a regulatory sandbox patterned on that developed by the UK's Financial Conduct Authority, in which fintechs can experiment with new solutions without immediately incurring all the normal regulatory consequences.

Your bank is an app

Monzo is a British bank created for the smart phone. The bank exists only as an app on your mobile phone. In addition to acting as a normal banking service, Monzo sends a message to your phone if you have overdrawn your account, reminds you to pay your bills, shows you how you are spending your money (when you have bought lunch at Pret a Manger ten times in the past month!) and keeps track of your receipts. Monzo's objective is to be a smart and foresighted bank that can provide assistance before you even know you need it.[8]

Lukewarm interest in banking services from Facebook and Google

In our survey, 79 per cent of respondents said they were not interested in using a helpful banking service from Google or Facebook.



[8] https://monzo.com/

Asked whether giving Google or Facebook access to their banking details (if they could offer a useful banking service) was problematic with respect to privacy issues, 87 per cent of respondents said yes. Of the 87 per cent who thought it was problematic, five per cent said that they would use such a service despite their reservations. The answers indicate that people are clearly sceptical about mixing their online social activities with banking services. Could this indicate that the banks have no immediate need to fear competition from Facebook and Google?

Eva – the invisible bank

KPMG has developed the future scenario "EVA – the invisible bank". [9] Eva is a virtual assistant that is based on artificial intelligence. It is fed with the bank's customer data and information the bank collects via partnerships with a supplier of a fitness tracker. It also has access to data from the customer's smart phone and social media accounts. Eva wakes you up in the morning, reminds you that it is your friend's birthday and asks if she can suggest an appropriate gift. At around lunchtime, Eva asks how you are feeling. You have eaten more junk food than you usually do, you have not been training for a week and you seem stressed, Eva says. Eva proposes that you take up yoga, and suggests a class that is held in your neighbourhood. "Yes, please, that sound fine", you answer, "Put my name down." "Perhaps Frode and Kari would also like to join your yoga class?" asks Eva. "I see that they have some free time in their schedules, and I think they would like yoga." "No", you reply, "I would rather go alone." "OK", says Eva, before telling you that she has switched your savings around a bit to obtain a better rate of interest.

[9] KPMG, "Meet EVA. Your Enlightened Virtual Assistant and the future face of the Invisible Bank", 2016

PRIVACY CHALLENGES

The services you use are becoming more personalised. Data about you is the new currency. Most people are used to and expect digital services and products that are tailored specifically for them. But how does it affect your personal privacy when banks, insurance companies and credit rating agencies have such a high consumption of personal data?

DO YOU CHANGE YOUR BEHAVIOUR WHEN SOMEONE IS WATCHING?

Everything we do online can be traced, sold on, analysed and used to deliver personalised services. More and more of our lives have been digitised, to the point where it can be difficult to keep track of who has access to data about us.

When the services we receive are based on our personal data, it is not hard to imagine that many of us will change our behaviour to obtain more attractive services. But it is also possible that we might avoid doing or saying things that could have a negative impact. Such a change in behaviour, prompted by the prospect of your actions having an impact on a specific current or future service, can be described as a “chilling effect”.

A life insurance policy that requires the policyholder to walk a certain number of steps each day may be perceived as push to exercise more. To some, this might feel like a helpful nudge in the right direction. But it is problematic for your individual integrity and self-determination if the device in your car records where you drive, and you no longer feel free to go wherever you like without someone looking over your shoulder.

COMPUTER SAYS NO

In future, more and more decisions about us will be made by algorithms instead of people. Automated systems based on artificial intelligence will determine the size of your insurance premium or whether your mortgage application is granted or not.

In many cases, this means more efficient and user-friendly services. But from a privacy point of view, the increasing use of smart algorithms constitutes a challenge. Many advanced systems based on artificial intelligence are like black boxes. The way the algorithms arrive at their results is so complex that they are difficult to understand. Which personal data about me does the algorithm possess, and how does it work?

There is one right granted to you by European data protection law that is particularly relevant here. The law requires companies to inform the individual to whom data relates (the data subject) about what personal data they are collecting and how it is used. The right to information is fundamental for privacy, but can be challenging for some service providers who use complex data systems that are difficult to explain and vast volumes of data that are difficult to account for.

THE MORE, THE BETTER?

Intelligent computer systems depend on data. The more data the system has access to, the more accurate and precise the analysis. Since much of our lives is digitised, huge amounts of data exist on us.

Fitness apps can say something about the risk you pose as an insurance policyholder. Information about how often your mobile phone battery runs down is used to assess your suitability as a borrower.[10] The law says that a business can only collect data that are *relevant* for the purpose of the service. In the time ahead, the question of where the line between what is relevant and not should be drawn will become even more pertinent.

[10] http://money.cnn.com/2016/08/24/technology/lenddo-smartphone-battery-loan/

Another challenge is linked to the almost limitless possibilities big data and artificial intelligence create for the analysis and use of data. By coordinating data from various sources, or putting together items of data that were individually meaningless, it will be possible to find connections and create personal profiles to a level of detail that has not previously been feasible.

Instead of starting with a specific purpose for which the necessary data is collected, the application of big data methods is often prompted by the search for a way to exploit data that the processor already has. This runs completely counter to the privacy principle that personal data can only be collected for specific purposes. As such, it constitutes a tangible problem that those wishing to use big data to personalise services must address.

LOSS OF CONTROL – WHO KNOWS WHAT?

It is impossible for today's digital citizen to have full control of her digital trace, to know who has access to her personal details and what consequences the data she generates could have.

Contributing to the confusion is the ongoing metamorphosis of the players involved. If Google eventually starts providing banking services, it could potentially collate an individual's banking data with data collected on them via YouTube, Gmail, Google Analytics and all the other services owned by Google. The Norwegian supermarket chain Rema 1000 now also offers insurance services, and recently launched an app which records all the items you buy from them. At the moment, there are no indications that Rema is using our shopping habits for insurance purposes, but the combining of roles can muddy the waters for the consumer.

In the banking sector, the revised Payment Services Directive 2 will contribute to the confusion. We will move from a monopoly situation, where the bank processes all our banking data, to a situation where we can share the same data with many different companies. This will require a great deal of openness and transparency on the part of the players involved, to ensure that customers understand what they are consenting to and can keep track of which companies hold what data on them. It is particularly important that these enterprises are open about how the data is used to analyse and profile the customers.

To prevent employee snooping, the banks have strict rules governing access to account information. Bank data can contain sensitive information about health issues, political affiliations and sexual relations. How will this be managed by small start-up businesses or companies like Google and Facebook?

We are seeing not only a slew of new service providers in the financial sector, but also that many major players are using the same broad definition of purpose as in this example:

«The data will be collected in order to develop the solution and provide you with a better service.»

Such a purpose gives companies colossal leeway to exploit the data they collect from users. This is unfortunate from a privacy point of view because the individual loses control over how their data are used.

LACK OF OPTIONS – BE TRACED OR PAY UP

As of today, we have merely seen the start of personalised automated services. This means that only a small number of people currently have an insurance policy based on the on-going collection of personal data, or an artificially intelligent personal banking assistant.

In the future, however, this type of personalised service will become more widespread. We could encounter a situation in which we are "forced" into solutions that monitor our lives in detail, either because there are no alternatives or because the alternatives are much more expensive. In our survey, around 70 per cent of respondents said they did not want to see insurance premiums based on detailed sensor-generated data about their day-to-day lives and behaviours.

We could arrive at a situation where the norm is that all those who allow themselves to be tracked will qualify for low-cost insurance, while those who either cannot or will not be monitored have to pay more for their insurance. People with little disposable income may then have no other option than to choose the cheaper products requiring surveillance. In this situation privacy loses because it costs.

DISCRIMINATION AND INCREASED SOCIAL INEQUALITY

Increased use of personal data to personalise services may have unfortunate consequences for marginalised and vulnerable groups of people. If physical activity is to determine whether you can have health insurance, and how much you spend shopping online is to determine your credit rating, which in turn decides whether you are allowed to take out a loan, already marginalised individuals or groups could find themselves having to pay more for certain services or being denied them altogether.

This type of intelligent system is based on pre-existing data on individuals or groups of people, which in certain cases could be affected by prejudice or imbalances. The algorithms themselves could also be biased, either due to their programming or because the data being entered skews the analysis or decision in a certain direction.

For example, Google's online advertising system showed men an advert for a high-paying job far more frequently than it showed the advert to women. Researchers have also revealed that adverts for consumer credit have been shown exclusively to people living in low-income neighbourhoods.[11]

[11] The New York Times, "When Algorithms Discriminate", 9.7.2015, http://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html

THE PATH AHEAD

New data protection legislation goes into effect in Europe in 2018. This legislation will have a major impact on the development of new types of data-intensive service.

The individual's control over their own data will be strengthened, not least through the right to data portability. At the same time technology advances in a direction where it becomes increasingly difficult to understand how computer systems arrive at their results. The General Data Protection Regulation (GDPR) meet this challenge by introducing two rights that aims to safeguard the verifiability of algorithm-controlled decisions, namely the right to an explanation and the right to object to automated decisions.

GREATER CONTROL OVER ONE'S OWN DATA

The right to *data portability* is a new entitlement that comes with the GDPR. A user is entitled to *obtain* a copy of all the information they have provided to a service, and to have this data *transferred* to another service. The objective of this right is to strengthen the individual's ownership of and control over their own data. It may also become an important means of encouraging competition between entities for the provision of privacy-friendly services.

Companies in possession of complex data sets and analyses of individuals may encounter practical challenges with regard to handing these over in a format that can be transferred to another service. For this reason, companies that collect personal data must already now start planning how they will meet the requirement for data portability. The requirement for data portability also means that companies which provide digital services must be able to *receive* data that customers bring with them from other services.

The new data protection regulation further enhances existing rights, including the requirement relating to consent and the right to have data deleted. Businesses must draw up statements of consent that people understand. Open-ended phrases of the type «We will use your data to improve our services» will not be accepted. Such phrases do not give users a sufficient understanding of what the data will be used for or any way of foreseeing how they will be used in the future.

The right to have your data *deleted* is emphasised through the «right to be forgotten». An individual may, at any time, withdraw their consent to the collection of data on them, and may demand that any and all data already collected be deleted. Businesses that collect large volumes of personal data must ensure that they also develop routines and programs that facilitate the deletion, inspection and transfer of all data. The collection of large volumes of data also has a cost element.

CAN THE BLACK BOX BE OPENED?

Many advanced systems based on artificial intelligence are like black boxes. The way the algorithms arrive at their results is so complex that it is incomprehensible to the human mind. Before they grant access to data about themselves, people must trust that the systems process the data in a proper manner, and that any decisions made are fair. The issue is whether we can trust completely automated systems, and how transparent an algorithm-controlled decision-making process can be.

If a private organisation is not trusted, people may be less inclined to share data about themselves or they may decide not to use a service or product.

To safeguard citizens' rights, it is therefore important to be open about the assessments and choices on which decisions rest, which data have been used and how these data have been collected.

Several countries are discussing how their inhabitants can obtain an insight into automated decision-making processes. France, for example, has considered a legislative proposal regarding digital rights and algorithmic transparency.[12]

RIGHT TO AN EXPLANATION

The new General Data Protection Regulation (GDPR) establishes two rights which are particularly interesting with regard to the development and deployment of artificial intelligence and automated decision-making. These are the right to object to automated decisions and the right to an explanation.

The GDPR entitles the citizen to object to his or her data being processed solely by a machine. This means that a person can demand human involvement in a decision-making process that will have an impact on them. However, there are several exemptions from the rule. This includes situations where the method of processing is provided for in law or where the decision does not affect the citizen to a material degree. Given the fact that the list of exemptions from this rule is long, it is uncertain how significant this right will be in practice.

The «right to an explanation» is more important and will probably be of greater significance. If you are subjected to an automated decision, the GDPR entitles you to be given an explanation of the logic underpinning it. This highlights the necessity of people being able to understand how the algorithms work.

It may seem obvious that people must be able to understand and explain the workings of the algorithms they themselves have developed. But the development of artificial intelligence has so far focused primarily on the actual *results* the algorithms produce, and has been less concerned with *understanding* how the results have been arrived at.

The legislative insistence on the «right to an explanation» is now inspiring research environments to develop systems that illuminate the logic behind the algorithms. MIT has set up a research project that aims to provide people with greater control over algorithm-based decisions. They are looking at how they

[12] http://blogs.lse.ac.uk/mediapolicyproject/2016/04/22/algorithmic-transparency-and-platform-loyalty-or-fairness-in-the-french-digital-republic-bill/

can make the algorithms more open and how they can enable people to obtain greater control of the outcome of the decisions the algorithm generates. [13]

TOUGHER STANCE TOWARDS GLOBAL GIANTS

With its 500 million consumers, the EU is one of the most important markets for US companies. However, EU decision-makers have started to look critically at how US companies are dominating the digital world.

In 2016, the following issues raised their heads:

- The EU accused Google of unlawful favouritism towards its own digital services at the expense of its competitors' on its Android platform.
- The French data protection authority ordered Google to implement the «right to be forgotten» globally across all domains, and not just at domain level in the EU.
- The EU accused Facebook of misinforming the competition authorities in connection with its acquisition of WhatsApp. Facebook stated that it would keep personal data about WhatsApp users separate from data collected via Facebook's online community, something it later went back on.
- Data protection authorities in France, Spain, Germany and the Netherlands are investigating the lawfulness of Facebook's collection of data from non-members.
- The French and German competition authorities are investigating whether Facebook has abused its dominant market position in the way it collects and processes personal data.

Things will not get any easier for US companies in the time ahead. With the introduction of the General Data Protection Regulation (GDPR), US companies will have to comply with European privacy legislation. The GDPR compels organisations domiciled outside the EU but offering goods and services to EU citizens to comply with the new regulatory framework. Organisations that do not comply with the new regulation risk paying heavily for their failure to do so. After 24 May 2014, violation of the GDPR will cost businesses up to EUR 20 million, or 4 per cent of their global annual turnover.

[13] http://news.mit.edu/2016/making-computers-explain-themselves-machine-learning-1028