Insurance & Pension Denmark

Data use and data ethics

Dilemmas and possible positions for the insurance and pensions industry

NEXTWORK

TABLE OF CONTENTS

NEXTWORK

Made by Mads Hennelund, Brian Due and Jesper Højberg Christensen for Insurance & Pension Denmark.

Executive summary

The focus of this report is on ethics with respect to collection and use of data within the insurance and pensions industry. It is motivated by the fact that today, and even more so in the future, we shall be able to collect and use even greater quantities of data for even more analyses, risk assessments, products and services. But simply being able to use data for multiple purposes does not mean that we must do it all.

This is a reflective think tank report, weighing dilemmas and testing potential ethical positions. It is based on several years of work aimed at mapping out developments within technology, data and social attitudes of particular relevance to the industry. The report was made by the strategy developers Nextwork on behalf of the industry association Insurance & Pension Denmark. In other words, the report is an external and unbiased assessment of data-related ethical concerns facing the industry based on a complex perspective of what is best for individuals, society and businesses.

The report is based on extensive studies of state-of-art literature, classical ethical dilemmas and discussions, interviews with industry experts and data experts from at home and abroad, interviews with members of Insurance & Pension Denmark as wells as workshops conducted with the board of the industry association. However, in this report we do not only sum up the opinions of others but contribute new models of data ethics, introduce a conceptual discussion and identify principles with which companies within the industry should concern themselves.

The main conclusions of the report are:

- Data represent the core of the industry's business models and, fundamentally, it is ethically justifiable, based on declarations of consent, to collect and use data for the benefit of customers and society with respect to risk assessment, prevention, compensation as well as anti-fraud initiatives.

- For the industry, three possible ethical positions are available. We recommend the actors of the industry to operate within what we define as position 2: The progressive position, which gives the customer control of the greatest number of personal data as well as the potential for benefiting from sharing of data.

- We recommend that the industry concern itself with all aspects of the ethical compass: Data security must be highly prioritized, and Privacy by Design should be an important principle. The customers should have maximum control of personal data, and their data should neither belong to operators or the public authorities. Personalizing risk assessment may create far more fairness in the market and should be used to benefit the customer if there is a fair and realistic alternative to those who do not wish to share many data. Behavioural adjustment and prevention based on increased data-sharing offer great opportunities and is ethically justifiable if real alternatives remain. It is also ethically justifiable to collect, use and store data and to offer policyholders incentives to give true information to the insurers and refrain from defrauding the insurance community. High transparency of data use – especially with respect to risk assessment – and transparency with respect to what the policyholder has consented to should be given high priority.

Dilemmas and possible positions for the insurance and pensions industry

Discussions about data ethics are typically sparked off by worries about the quantity of data. It is debatable whether we should delimit ourselves from using or minimize the use of data. We might call this a data-minimising approach to data ethics. Limiting the use of data may be justified by many good arguments, but primarily it is a matter of giving individuals the possibility to protect their privacy vis-a-vis organizations or companies, should they so wish. But, equally, there are many good arguments for using more data, what we have termed a data-maximising approach. First of all, it is about enabling customers, through use of multiple data, to achieve more accurately tailored products and a fairer price.

However, it is not a question of either or: More or fewer data. Because it is possible to minimise data use for many different reasons: From the perspective of concern for individual privacy or concern for the very social contract and trust between individual, society and business. Secondly, the matter of data is far from unambiguous for the individual and the creation of value. There are major nuances and differences of crucial importance to data: are they personally identifiable, are they a matter of statistics, are they figures in excel sheets or behaviour on social media? Are they sensitive and personal or insignificant; have data been consciously provided or are they a product of behaviour that may easily be combined, shared and used, or is the quality of data poor etc. Reflections on data ethics should go deeper than merely discussing minimising vs. maximising approaches. And many might, perhaps, also take the position that the use of data is a matter of combining the two. Concern for the individual is a precondition for trust, which is an asset the industry may use to create value for the individual. In such a value-and-trust cycle it may, perhaps, not be so much a matter of how many or how few data are being used but about relations with customers.

In this publication, we assess and discuss three positions of data ethics and the dilemmas posed by each.

THE CRITICAL POSITION:
The individual should own all data and we must limit our use of the data.

THE PROGRESSIVE POSITION:
By giving consent the individual may benefit a lot from use of his or her data.

THE OFFENSIVE POSITION:
We use everyone's data for the benefit of all.

Our reflections on data ethics should be seen in the light of the business models of the insurance and pension industry, the international competition - which influences the way Danish companies use data - the consumers' wishes and demands on the industry as well as basic ethical principles. Naturally, it is not up to the industry alone to decide on ethics. We can choose to stay more or less ahead of or behind the cultural developments and norms of society. But we also know that norms are culture and context specific and that they change over time. So, if customers, with respect to data use, move in a direction that the Danish industry has defined as unethical, foreign competitors may still be able to compel Danish operators to follow suit and discard obsolete ethical principles or the other way round. For the industry, data ethics will always be a question of individual, society and business.

We know that the new data sources may affect the value chain from distribution, customer acquisition, marketing and targeting to underwriting and pricing, pooling of risks, handling of claims and disbursements, prevention of claims or harmful behaviour to cross-selling, upselling etc. Combined with increasing capacity in the companies to collect, analyse and store large quantities of structured and unstructured data, many new

Prime Minister of Denmark Lars Løkke Rasmussen used the occasion to express his appreciation of the fruitful cooperation between the Government and Insurance & Pension Denmark. "This is my clear understanding and experience from the governments I have been part of", the Prime Minister said from the podium. "I wish that data ethics becomes a competitive advantage for the Danish business community", the Prime Minister added.

possibilities for value creation will emerge for both operators and policyholders. But the new opportunities for value creation also entail new problems in terms of monitoring, privacy, behaviour regulation, segmentation etc. At the same time, the massive development within technology and increase of data also present a number of solutions that we may not yet be familiar with, but which may make today's problems appear negligible tomorrow. Therefore, we do not propose to present easy answers. For ethics is always a balancing act, and dilemmas are unavoidable.

This think tank report is based on interviews with industry actors and experts, research, existing knowledge within the team of writers as well as input and evaluations from around 250 participants at the industry's annual meeting on 15 November, 2018, on the theme of data ethics.

#data ethics

Towards a common data ethics at the annual meeting of Insurance & Pension Denmark, 2018

"We might well sit back and protect ourselves, but that's going to be like the man ringing a bell in front of a car to make sure that it didn't frighten the horses. We need to take care that we do not crawl into a hole, believing that the rest of the world stands still, because we do not want to share data. So, the task for us will be how to share data and protect them by drawing an ethical line. How do we set the limits and what commitments do we make to each other? To protect the data we use – and we will be using them – we will use them within an ethical framework that we can all agree on. It will be difficult to put into writing, but, then, that's what we must try to do." – Søren Boe Mortensen, Chairman of the board, Insurance & Pension Denmark.

The data explosion and the need for a carefully considered position on data ethics

"We are going to see some quantum leaps in the time to come in terms of what we can do with data, and in this context, it is probably more important than ever to sit down and decide how we are going to operate in that world. What rules and principles will we be pursuing?
– Thomas Ploug, professor at Aalborg University and former member of the Danish Council on Ethics.

For centuries, civilised societies have collected and used data. Take Joseph and Mary, for instance. They went to Bethlehem because "all the world was going to be taxed". It was burdensome, but we have come far since then, and with accelerated digitalization we can now retrieve useful information much more easily. We get access to even more data, even more data sources, even more methods of data collection, even more sophisticated tools for analysing data and, consequently, even more possibilities for using data to understand policyholders and citizens, to predict their behaviour, make risk assessments, market products and offer personalized services and products. We can do a lot with data. But what should and must we do – and perhaps refrain from doing?

"It is important for industries to develop a codex on what they intend and don't intend to do, and I am convinced that it is through the process of developing such a codex that we will achieve the greatest value; that we will reflect on these matters and feel the different, difficult choices."
– Povl Heiberg Gad, Ph.D. student at CBS

Data may be used for good or ill – that's why ethics are important

Since the first insurance policies were taken out, data have been an integral part of operating insurance business. In the year 3.500 BC, Mesopotamians began recording data on clay tablets. In those days information about trading transactions, professions etc. was recorded on the tablets. In the vast majority of cases registration has been to the benefit of the citizens – then as well as today. For registration of data enables correct tax collection, for instance, thereby minimising tax fraud. Also, registration was and remains necessary to ensure correct hospital treatment. And, moreover, with respect to issuing of ballot papers, which help keep democracy going. But historically, too, data have represented a potential and at times quite real threat. During WW II, for example, registrations from the synagogues proved an efficient tool for identifying and capturing Jews (Rahman, 2016)

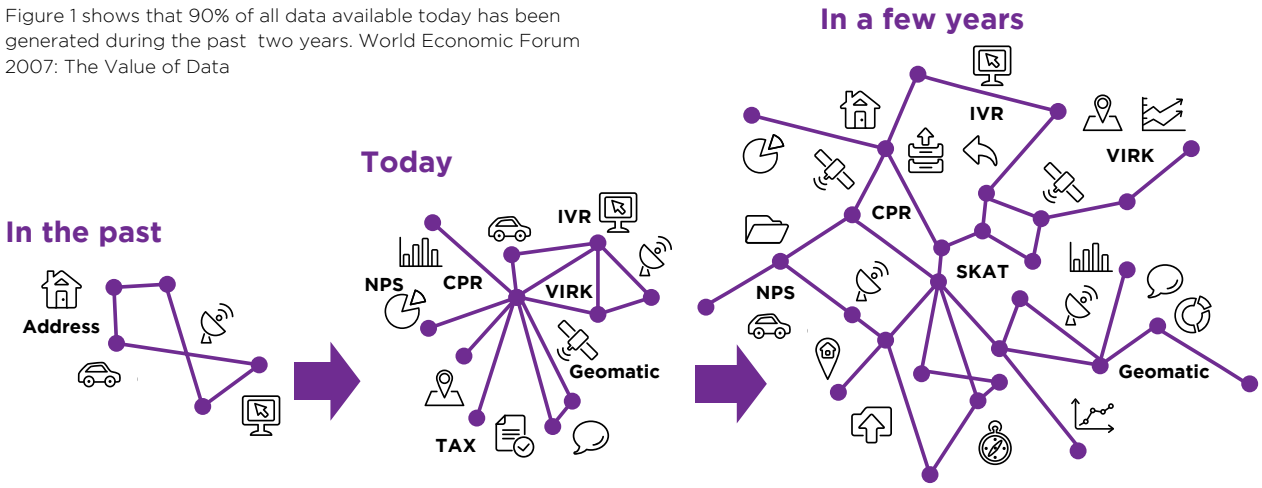
So, data are not inherently good or evil – it all depends on the way they are collected and used. For this reason, ethics are extremely important, because data may be used for bad purposes, but also uncritically and in an unreflected way. And even if you have no unethical intentions, it is possible – as the German philosopher Hanna Arendt (1994) has demonstrated – simply through lack of judgment and responsible reflection to commit unethical acts (Due, 2018).

The volume of data will increase no matter what the industry chooses to do

Data are and remain the foundations of the business model of the insurance and pensions industry. If the operators refrain from using data to pool risks, there will be no insurance business. If the pension companies do not use data to ensure the best possible coverage with respect to the individuals' financial position and desires in life, the result will be greater insecurity about life after the labour market. Data are the valuable foundation, and that's always been the case.

"We are going to see some quantum leaps in the time to come in terms of what we can do with data, and in this connection, it is probably more important than ever to sit down and decide on how we are going to operate in that world. What rules and principles will we be pursuing?"
– Thomas Ploug, professor at Aalborg University and former member of the Danish Council on Ethics.

Figure 1 shows that 90% of all data available today has been generated during the past two years. World Economic Forum 2007: The Value of Data



Data are evidence of occurrences. They reveal behaviour. Unlike oil or gold, data are not a scarce resource – even if some mistakenly use that metaphor. For data can be stored in physical locations and forever. And data bases will not get any smaller if more people use them. Fundamentally, data are raw figures/numbers that through analytical processing are turned into information and subsequently, through more advanced interpretations into knowledge enabling us to act and make decisions (Davenport & Prusak, 1998). This is not a new phenomenon.

What is new is not that the industry collects data. Rather, it is the extent and categories of data that are collectable for the industry as well as the potential for combining them in completely new ways through advanced IT processes. A new element is also that software robots increasingly are able to collect data themselves, analyse them and make decisions on that basis. This constitutes a radical change. Because what will it mean to customers and operators if robots increasingly are able to make ethical decisions, for instance about requiring a higher premium from Mr Jensen than the one charged of Mr Hansen based on health data, welfare data, social media data, data revealing driving behaviour, drone surveillance etc. With what principles should the software robots be encoded?

What type of data should be used? How many? What types of decisions should and can be made? We need strong commercial, ethical principles to handle and legitimize such decisions.

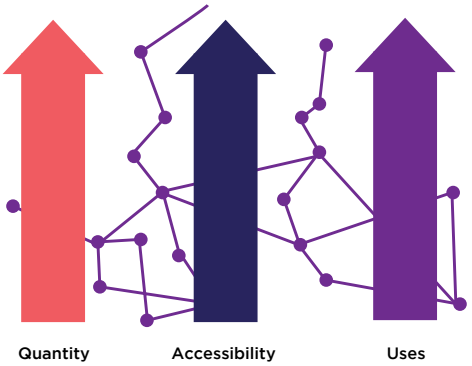


Figure 2 shows that not only will the quantity of data increase. Data will be more available, and the number of possible uses will continue to increase.

Data ethics is an element of the operator's general ethical responsibility

Ethics is not a new challenge for operators in the industry. "Unethical acts" have always had the potential to generate crisis and have required issue management. Taking an ethical stand on data collection and use, therefore, should not be seen as something radically new but as a continuation of the ethical operator's position in society. As with a high level of employee satisfaction and impressive green accounts, the companies of the industry can use a position on data ethics to databrand themselves (Due, Christensen, & Hennelund, 2018). And just as dissatisfied employees, environmental pollution or failure to follow up on grand promises will lead to crisis and risk of greenwashing, lack of data ethics may generate major problems for the industry, and pronouncements on data ethics without subsequent action may lead to accusations of ethics-washing (Wagner, 2018). Ethics-washing is when companies, in their principles and on homepages, make ethical claims without making actual ethical decisions in their daily work. Obviously, this is unfortunate. Therefore, the intention of this report is to set the stage for reflections on data ethics within the industry that will also lead to vigorous execution.

"Conflicting" expectations and views among policyholders

Today, there is broad political support for protection of personal data and for the individual's ownership of personal data. Furthermore, there is a commitment to reducing and simplifying access to public data bases and registers. Around the world we see new companies working with encryption of personal data and statistical techniques aimed at minimising information at the level of the individual *(differential privacy/traceability).* It is a matter of allowing the individual control of his or her data and of identifying the value of data. But among the policyholders of the industry we encounter conflicting expectations of how data should be used. An example of this is the conflict between solidarity and fairness, where new uses of data challenge solidarity while enabling more individual fairness.

Policyholders want privacy
Socially and in society in general there is increasing awareness of privacy, and it is as consumers that policyholders make more idealised demands of the operators' use of data. Millennials are likely to attach greater importance to – and instantly be able to decode – whether an operator, organization or authority is trustworthy, in possession of a solid, comprehensive set of values and offers sufficient advantages in return for personal data.

Policyholders want a business model based on 'solidarity'
A more accurate and risk-based price is often seen as conflicting with the insurance principle of solidarity under which policyholders jointly cover each other's risks. This principle of solidarity is often associated with what is termed systematic redistribution, where everyone in the insurance pool in principle ought to pay the same for their *systematic risk*, a solidarity that we accept with respect to the welfare state. However, the solidarity in insurance is a matter of massive unsystematic redistribution from those who suffer no misfortune to the few unfortunate ones who do. Still, this does not alter the fact that greater personalization of insurance products is typically associated with backing away from solidarity. However, this is not a law of nature.

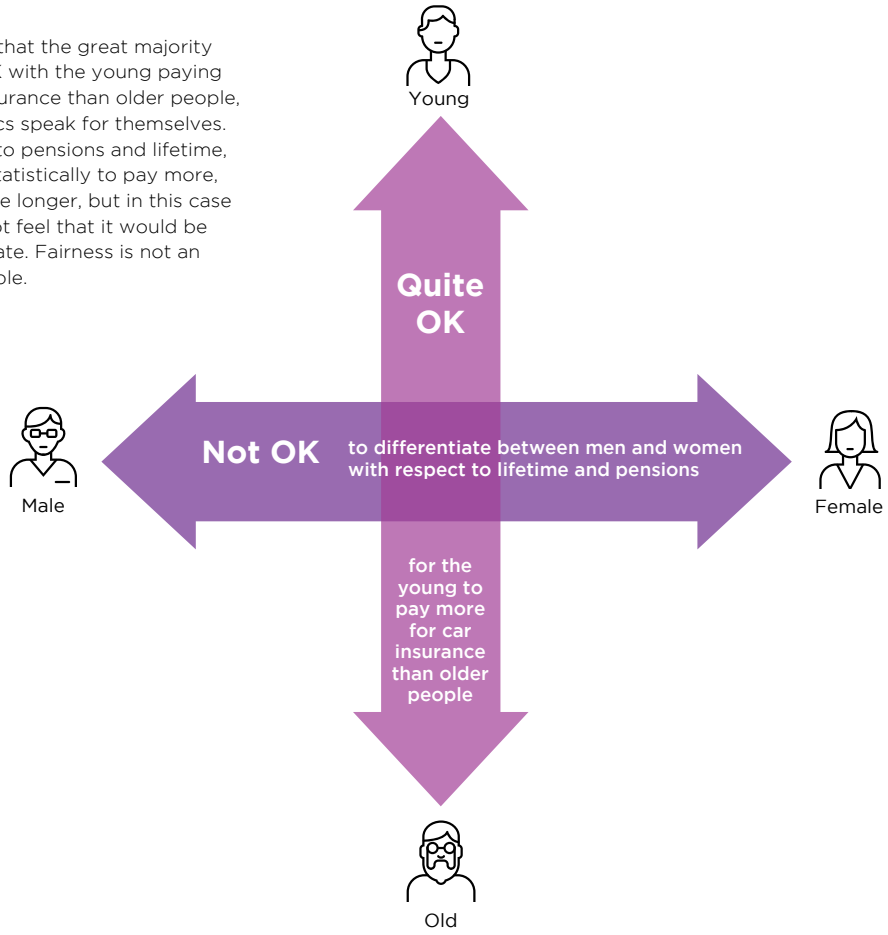
Policyholders want a fair, risk-based price, promptness and service
Policyholders also want a 'fair price' based on their actual risks (data). The elite driver who has earned points for good driving does not want to pay the same as the youngster who has just obtained his driving licence. Additionally, advanced data analytics combined with AI offer great opportunities for creating better customer experience with respect to insurance, from marketing, onboarding and customer service to claims management and disbursement. Customers want these, especially if they result in cheaper premiums. So, while policyholders on the one hand focus more and more on privacy, they are also "quite lazy" and price-conscious – as behavioural economics has shown time and again (Thaler & Sunstein, 2009). So, if customers get something valuable in return for providing data, many view this as a good deal. A study by Accenture has recently shown that 83% are willing to share data in return for a more personal experience.

Customers accept some forms of differential treatment

Naturally, the culture in society influences ethics. We accept a basic differentiation between young and old when it comes to car insurance, because statistically the young are worse drivers than the more mature. On the other hand, we do not accept asking women to pay more into their pension schemes because, statistically, they live longer.

Age discrimination is OK, it seems, but not sex discrimination. It is quite in order that fast and large cars are more expensive to insure, but it is not OK for the academic who eats healthily and exercises daily to pay much less than the worker who has a different and apparently riskier lifestyle. Such pragmatic matters are not necessarily economically rational, but they reflect universal perceptions that may be integrated within ethics.

Figure 3 shows that the great majority of Danes are OK with the young paying more for car insurance than older people, because statistics speak for themselves. When it comes to pensions and lifetime, women ought statistically to pay more, because they live longer, but in this case the Danes do not feel that it would be OK to differentiate. Fairness is not an 'objective' variable.



While ethical principals remain firm, moral standards change over time

In chapter 2 we shall go into greater depth with ethics and ethical positions. But, basically, we follow the common definition of ethics as a system of principles and morals; as the norms that apply in practice at any given moment. The ethical, Kantian principle of not treating any human being exclusively as a means to an end, however, is defined differently in different epochs and cultures.

Human life is inviolable, but when it comes to concrete, every-day situations, dilemmas abound. A good example of an ethical dilemma that can be traced all the way down to the specific encoding of an algorithm is the question of driverless cars.

Studies from MIT, published in Nature (Awad et al., 2018) – based on a global survey of people's moral position on a number of dilemmas relating to driverless cars – show that there are quite large cultural differences. If, for instance, a car cannot avoid hitting either an older or a younger person, considerable differences emerge: In the East, the preference is for hitting a younger person (e.g. Saudi Arabia, China, India). In the South, on the other hand, they would prefer hitting the older person (e.g. Southern Europe, South America). Finally, a more equal distribution is found in the West (Europe, North America). All agree on the principle that human beings are inviolable, but forced to choose between two evils, you clearly see different societal norms emerge. Apart from showing that the question of driverless cars is challenging to the insurance industry, both in terms of life assurance and car insurance, it is also a good example of how ethical principles are interpreted differently in different cultural contexts based on different norms.

> *My car, my home and now my health insurance policy are IoT-driven. The health insurance policy is from an operator that has used Big Data to completely change the life and health model. They looked at where the health insurance sector was going. They felt this was a model which - in terms of private medical insurance – was going to become difficult for insurers and largely unaffordable for consumers as well. So, they thought 'Let's model what's happening' and instead of paying claims for health insurance and paying out early on life policies, let's try to prevent it by encouraging healthier life styles'. They do this by monitoring my exercise activities using the standard health monitoring devices that many people use already and offer rewards and reduced premiums for maintaining a healthy lifestyle.*
> – Norman Black, EMEA Insurance Industry Principal, SAS

The fathers of anthropology and sociology – such as Clifford Geertz (1977) and Emil Durkheim (1895) – have shown that societal norms are dynamic and change gradually as new developments take place. We are already experiencing what has been called the fourth industrial revolution (Schwab, 2017) with radical digitalization also impacting on our norms. Therefore, it is to be expected that attitudes to what data represent, are and may be used for will change over the years to come. But how and in what direction is impossible to say.

We shall probably see many simultaneous changes in various directions. Until quite recently, the significance of data was relatively unknown among the population at large. But with cases such as Facebook/ Cambridge Analytica, and following the introduction of GDPR, far more people have become conscious of what data are and may be used for. This entails greater critical assessment and deeper understanding of their potential.

The industry is not alone in the international field

Even though people today are much more conscious of data than just a few years ago, many continue to have only a quite superficial grasp of data. As we have already discussed, it is far from given that more data will be ethically wrong and less data ethically good. This type of dichotomy is not productive and is based on an unsubtle understanding of data. Using more data can save lives but also potentially harm the individual. A lack of understanding and a crude approach to the debate on data use may prevent us from seeing and developing business opportunities that we hardly recognise today – business opportunities that in the greater scheme of things may also be more ethical. Thus, fear of getting involved in the matter of data may result in competitive weaknesses, in a global perspective, where foreign companies may develop ethical solutions and products for customers that the Danish industry refrains from taking up. As a result, foreign players will arrive and capture mainly the 'good part' of the market, i.e. policyholders who, perhaps, already benefit the most from sharing data. Within the field of personal insurance, these are likely to be the best-positioned low-risk groups.

> *There will be a cultural movement with respect to what is OK and what is not. But in the future, you do not need to be insured in Denmark – there are companies in the world, and outside the EU, that rely much more on IoT. And this will happen! Not in 10 years, in 5 years more likely, putting pressure on Danish operators, because the foreign operators will capture the 'the super insurable'."*
> – Jon Jonsen, group CEO and & COO of PFA (pension operator)

We are already seeing it today within the market of leisure boat insurance. Most boat owners keep their boats in Danish harbours while taking out their policies abroad.

Here the foreign insurers win on price, one reason being that in Denmark we pay a tax on hull insurance. As we cannot keep out foreign entrants in a global world, we must – from a commercial perspective – be able to meet the competition and use far more data points. But it is not only commercially rational. It is also ethically rational, because in Denmark we have societal regulations and corporate cultures adapted to Danish conditions, whereas foreign entrants may not share the same ethical standards. Not only is the industry coming under pressure from international actors able to offer cheap and personalized products, new super digital players, e.g. from insurtech and fintech, contribute to influencing the norms of the policyholders as to what is OK – and even expected of the operator you are interacting with. Innovators outside the industry, such as Amazon, influence the policyholders' expectations in terms of monitoring and intelligent use of data, because they have demonstrated that these result in better services.

The picture shows chairman of the board of Insurance & Pension Denmark and CEO of Alm. Brand, Søren Boe Mortensen, on the stage at the annual meeting of Insurance & Pension Denmark, which was about data ethics

Debat on foreign competition at the annual meeting of Insurance & Pension Denmark, 2018

"It does mark you out as a fool if you don't fear an operator that has a good grasp of its customers and many data points. Amazon, for instance, has 2000 data points about its customers, so, naturally, it is a threat."
– Lars Bonde, COO, Tryg

"There is no doubt that they will be able to provide products that are not available today. It is not something that is keeping us awake at night right now – but that may come later. But basically, as a foreign operator, you must observe legislation on data protection as well as other Danish legislation. Now, whether it is being enforced is a different matter, and I do believe we need to pay attention to, perhaps, putting up some different fencing posts around what we'd like to see happen in Denmark."
– Anette Høyrup, senior legal adviser and privacy expert, the Danish Consumers' Council 'Tænk'; deputy chairperson, the Danish Council for Digital Security.

Investment robots such as June, Darwin and Sparindex may also affect the customers' view of combining and producing data, financial overviews and transparency. These, again, may affect expectations of what pension operators ought to be able to do, and how many financial data you are prepared to keep together within one single universe – in one place. Increasing awareness of investments and ethical investment pools also makes demands of what pension companies can and should offer their customers. And such innovations are naturally driven by what is technologically possible. Perceptions of what is creepy and unethical are generally changing in the sense that what once was "too much" is now seen as desirable or almost to be expected. But more scandals, such as the Cambridge Analytica affair, which have resulted in such outrage among the consumers, may result in an actual counter movement – a techlash – where people become very conscious of their own data and the behaviour of others.

The industry has been good at mapping behaviour and risks via data and methods of data analysis. Today the industry holds even more data. The enormous potential this represents to individuals, companies, the public sector and the government – if data are used sensibly – should continue to receive the industry's support. Rather than shutting down and putting up boundaries, we have opened up for a dialogue between the industry and its stakeholders (citizens, politicians, authorities, interest organisations etc.) on the possibilities of the digital world. To frame this discussion even more accurately, we have been working with three different positions on data ethics.

Three positions of data ethics

We have experienced that the debate on data ethics often divides people into two different camps. On the one side are the enthusiasts who can barely contain their exuberance about the endless potential of data. They see data as a free-flowing and untapped asset that represents commercial potential, especially if you can aggregate data and add even more value to them, ultimately leading to innovation. On the other side are the privacy champions advocating consumer protection, insisting that the citizen must take priority to the system and the operators. They see data as a private asset that must be treated with great respect by operators and public authorities – especially sensitive personal data. Both sides have different views of what data and data ethics are and should be. Therefore, we need to distinguish between ethics of duty and utilitarianism.

Where ethics of duty is about not placing the individual as a means to an end – because all individuals must be treated as ends in themselves – utilitarianism is about increasing utility value for as many as possible. Utilitarianism, moreover, may ethically defend doing so at the expense of the individual, something ethics of duty will not allow. The two ethics represent a fundamental conflict in the history of ideas.

Ethics of duty may be traced back to philosophers like the German Emmanuel Kant (1785) who proposed the categorical imperative: "Act only in accordance with that maxim through which you can at the same time will that it become a universal law." And in the second formulation: "Act in such a way that you treat humanity, whether in your own person or in the person of any other, never merely as a means to an end, but always at the same time as an end". To sum up: according to the ethics of duty, it is an ethical duty to give priority to the individual human being.

Utilitarianism is not necessarily the opposite of an ethics of duty, but its focus is completely different, i.e. on what benefits the largest possible number of human beings. Utilitarianism may be traced back to political philosophers like Jeremy Bentham and John Stuart Mill. Originally, it was about ensuring happiness and good fortune for the greatest number of people (Bentham, 1776), but in more recent versions it has been put forward as rule-based utilitarianism emphasising that rules must be established to ensure optimization of the happiness of the community at large.

If we juxtapose the two ethics, it turns out that there is a difference between setting out to advocate the rights of the individual or the possibilities of the collective for better services and quality of life. However, they are not as mutually exclusive as they are often claimed to be, especially in debates concerning the industry's access to data.

GDPR is an example that the demand for better informed and transparent declarations of consent – i.e. concern for the individual – can and should be maintained as a partial precondition for compa-

nies creating utility value for the greatest number of people. Also, more accurate risk assessment may be what is most fair to the individual, for one thing because the price would be much lower, and perhaps also being of benefit to society in general (utilitarianism), because personal funds are allocated more effectively, and the loss of welfare is minimized. So, if, as a matter of principle, there is definitely a difference between arguing from the point of view of either ethics of duty or utilitarianism, it is possible, from a more pragmatic perspective, to discern an overlapping of the positions.

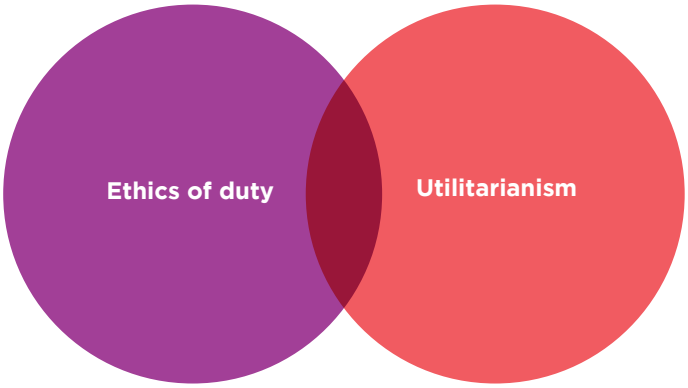


Figure 4: The possible overlapping of an ethics of duty and utilitarianism

> *Basically, if you respect privacy, you keep within the circle representing ethics of duty. But if you are within the all black area with respect to utilitarianism, you are outside the circle. This is the balance you must consider."*
> - Povl Heiberg Gad, ph.d.-stipend at CBS

You may then ask if ethically justifiable targets (in terms of ethics of duty or utilitarianism) may be achieved by refraining from making use of data? Or whether ethically justifiable targets may be achieved by using more data? These questions may also be placed on an axis as shown in figure 5

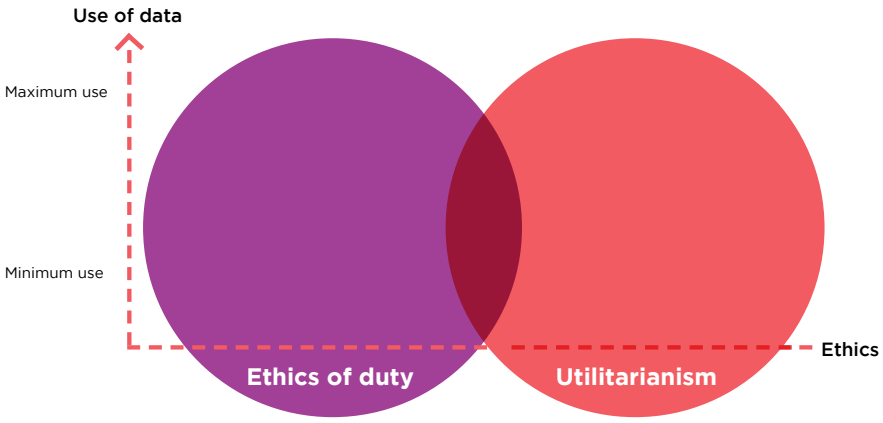


Figure 5: The Y-axis shows respectively maximum and minimum use of data. Generally, there will be a tendency that, the higher you proceed up the data-axis, the more innovation and development will be required with respect to privacy by design (PbD), data cleansing, organization and encryption. Several of these innovations have not been fully developed, and for this reason uncertainty grows proportionally the higher up the data-axis you move. Greater use of data typically also requires somewhat greater efforts with respect to convincing others that what you do is good and proper. And there may be a tendency that what you do not quite understand is given the label 'probably dangerous'.

Outline of the three ethical positions

So, responses to the different ethical dilemmas and themes that emerge may be based on different ethical positions (ethics of duty and utilitarianism) and approaches to use of data (more v. less data). This is manifested in three fundamental ethical positions.

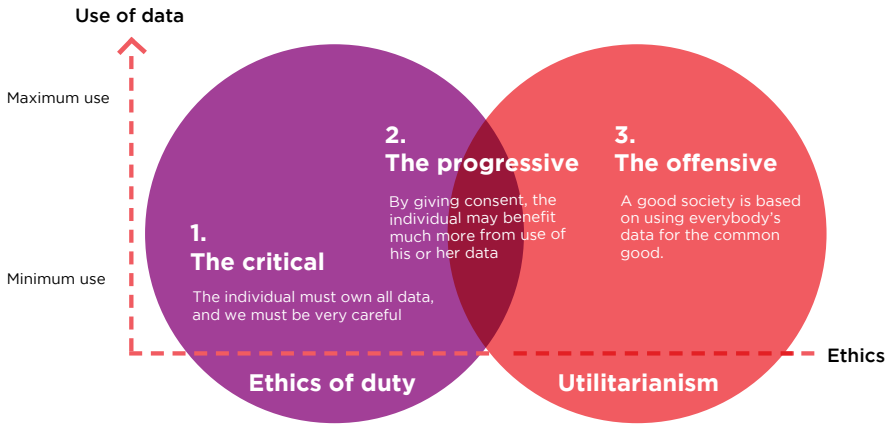


Figure 6 shows the three positions of data ethics. From the point of ethics of duty versus utilitarianism and maximum use of data versus minimum use, three different positions of data ethics emerge. A position based on ethics of duty and minimal use of data and two of maximum use of data which differ from each other in terms of the ethical point of reference.

The three positions may be described as follows:

Position 1 - The critical:
The individual must own all data, and we must be very careful
Here individuals and operators will argue for limiting collection of data and for deleting data out of respect for privacy.

Position 2 - The progressive:
By giving consent, the individual may benefit much more from use of his or her data
Here individuals will assume ownership of their data and create value for themselves, and the operator will support this for the benefit of the customers and the operator itself.

Position 3 - The offensive:
A good society is based on using everybody's data for the common good
Here the operator may want personal data to benefit innovation and for the good of society. And this must take priority over concern that a data point may ultimately be linked to a specific individual. The most important is not that the individual should assume ownership and put data into play but, rather, that data should benefit as many as possible. This common utility value will often be looked after by one of the institutions of society, such as an insurance unit, but may also be handled by a private business.

The model, then, provides three different positions with different consequences. In the following, we shall elaborate further on these positions.

Position 1 – The critical: The individual must own all data, and we must be very careful

Position 1 first and foremost focuses on privacy of individuals. In this position individuals and companies will argue for limiting collection of data and for deleting data out of respect for privacy. Polemically, data collection and use are seen as monitoring of individuals. Data should only to a limited extent be collected, stored and used. Those taking position 1 are typically consumer organizations and critical intellectuals. Position 1 is probably the most dominant in the media today and has acquired additional support following cases such as Facebook/Cambridge Analytica. Advocates of position 1 will especially focus on the individual being and end in itself and that it must never be a means to achieving other ends.

Consequently, it will never be acceptable to sacrifice an individual's private data – without active consent – to the advantage of any given utility value. Whether it is a matter of a slightly better product or knowledge that may save 100 lives, the individual's control of and right to limit the use of personal data must not be questioned. In this position, thus, focus is typically on the negative aspect of data.

Personal data are about privacy, and that is something to protect. Phrases such as 'surveillance society', 1984, and "misuse of data" are often used in this position. But basically, it is also a matter of protecting the individual against threats from tech-monopolies, members of the industry with commercial interests or a government that values collective considerations over the individual's legal rights.

Commercial strengths

- The industry to a certain extent precludes itself from data-driven innovation and development and compliance with consumer demands for products based on risk assessment, knowledge, behaviour, life situation and needs.
- Policyholders may actually experience inquiries from their operator as both 'creepy' and not least disturbing if fewer data are used on needs, life situation and previous dialogue about x, y and z etc.
- Risk of global competition affecting the Danish consumer market in a socially unbalanced way, resulting in only 'the best' getting cheap, personalized insurance from abroad.

Ethical opportunities

- Sensible position if large tech-companies cause more scandals, or when GDPR fines are revealed to the public.
- Always on the safe side in terms of various ethical recommendations, e.g. from the expert group on data ethics.
- Generally speaking, a risk-minimising position.

Commercial weaknesses

- The industry to a certain extent precludes itself from data-driven innovation and development and compliance with consumer demands for products based on risk assessment, knowledge, behaviour, life situation and needs.
- Policyholders may actually experience inquiries from their operator as both 'creepy' and not least disturbing if fewer data are used on needs, life situation and previous dialogue about x, y and z etc.
- Risk of global competition affecting the Danish consumer market in a socially unbalanced way, resulting in only 'the best' getting cheap, personalized insurance from abroad.

Ethical challenges

- Danish operators will lose business as foreign competitors, perhaps with poorer ethical standards, pick up the good parts of the market (natural selection), thus challenging principles of ethics of duty.
- Customers unable to get 'fairer' personalized prices and better service as this would require use of more data.
- Ensuring privacy via anonymising or deletion will prevent the individual citizen from sharing the value created by his or her data.
- Consumer protection may amount to protection of the insurance fraudster, which is a problem in terms of both ethics of duty and utilitarianism.

Position 1: Example

If policyholders Anne or Jens share many data with their insurance or pension operators, there is a risk that these data may be used against them, and a risk that data may end up in the wrong hands. Consequently, the best for Anne and Jens would be to protect their data above all. Therefore, they must be careful about using new data options and refrain from giving their operators access to more data. In addition, more data should be anonymised to ensure greater security and reduce the risk of misuse.

Position 2 – The progressive: By giving consent, the individual may benefit much more from use of his or her data

Position 2 is based on the individual owning data and the recognition that data are a public, commercial and private asset that should increase in both quantity and quality and be used as much as at all possible in order to create the best offers, services, assistance etc. for the individual. The message is that having many data about an individual and all other individuals may create benefits for all, but first of all for the individual. If position 1 is about formulating what happens, and what should not happen, then position 2 is far more about formulating what should happen but has not yet happened4. Data are viewed as an asset and as the basis for innovation and business. Not only because data create commercial advantages, but also because more data may lead to fairer prices.

> *More control of your own personal data will eventually determine how much you want to participate in the ever-growing digital economy as you get to control how private you do or don't want to be. If there are economic incentives to share data, we will see both economic participations increase in addition to new, more robust sources of data to better quantify and manage risk."*
> – Steven Schwartz, Managing Director, CEO Quest

This position places the individual at the centre as "data subject' and stimulates sharing of personal data. Today security and encryption of data, and solid mechanisms for storing and safekeeping of personal data, are not top notch. In the long term, GDPR will help ensure this, and the technological development and demands from customers will also accelerate the development. From the perspective of position 2, then, we look ahead and single out the potential and that technology will soon be able to offer great protection with respect to collection and storage of an individual's personal data.

Customers will increasingly demand and insist on getting control of their own data. The individual will then be in a position to put his or her data into play in the economy via transactions involving an operator requesting access to specific, personal data that it intends to use for x, y and z but not for q, v or w. Instead of compliance-consent by e-mail, it is about placing the individual at the centre of things and about his or her benefit from transparent use of data.

Position 2 is about maximising the value and use of data – but never at the expense of the individual – and, thus, this position aims to combine privacy and the maxim of utility by dissolving the conflict between the two opposites and placing them side by side. The ambition, then, is to bridge ethics of duty with utilitarianism, which, obviously, is uncomplicated. As a position the answer is always first and last that the individual's duty (and the individual's utility) takes priority.

> *If you leave the internet as it is without the seatbelt – the safety devices – then it is a question of either-or. Either you share data and get monitored or you have privacy. We try to remove the 'or' and replace it with an 'and'. You can share 'and' have privacy and security. The change that needs to be done is that we have to change the location or source of data being used. Today the companies hold, trade and use our data around us and it's actually not very efficient nor permissioned. The one entity that could potentially know all the facts about the individual is the individual itself, and that should be our starting point."*
> – Julian Ranger, Chairman & Founder, Digi.me

Position 2, therefore, also requires reading Article 20 of the GDPR on data portability as a unique possibility for giving the individual control of his or her data, and the possibility for sharing more data across organizations that might compete on value offers, security and transparency around specific parts of an individual's personal data[5].

Commercial strengths

- Better data-based pricing, customer service and counselling.
- Privacy by design as innovation and source of value creation.
- Focus on consumer as well as business concerns (GDPR).
- Enables further minimising of affectable risks and, hence, reduction of disbursements.
- The position makes it possible to stay competitive with respect to the surrounding world.
- Allows development of consumer tools that may stimulate inclusion of further data to the benefit of individuals and companies alike.

Commercial weaknesses

- The position presupposes several infrastructural elements such as transparency, high data security and a well-educated digital consumer, which may still be a somewhat utopian idea.
- The position makes very great commitments, especially with regard to data portability, which, again, may be difficult to live up to in practice.
- Data quality is important but difficult to guarantee.
- More data will pose greater storage challenges.

Ethical opportunities

- Compliant with ethical recommendations and the spirit of GDPR.
- Value may potentially be traceable to the individual and enable a more equal win-win relation between consumer and operator.
- More accurate pricing will permit far more fairness within insurance pools.

Ethical challenges

- Further personalization in terms of price may lead to 'discrimination'.
- Free choices, in the form of realistic alternatives, must be available if greater use of data, especially with respect to pricing, is to be ethically justifiable.
- The position will require solutions aimed at the weakest (claim based on ethics of duty) and taking a stand on the industry with regard to economic and social inequalities.
- Many automatically see 'more data' as 'dangerous'.
- The problem of pseudo-consent will become a great challenge.
- Digital education will become an additional obligation in order to get less digitally knowledgeable citizens onboard and enable sharing of advantageous and often necessary data relating to a claim.

Position 2: Example

If we, once again, take a look at Anne and Jens, they should be able to exploit the many possibilities offered by their data. Because Jens might get help to overcome his stress and back-related problems, if he so wishes, and Anne might get help to prevent water in her basement, if she so wishes. They may also get a more accurate price and a more tailored service if that is what they want. And, at the same time, sharing of data supports research and innovation, and for that reason, position 2 may potentially build a bridge between ethics of duty and utilitarianism. Anne and Jens must control their own data so that it will be up to them to decide which data to share and with whom.

#data ethics

The progressive position 2 up for debate at the annual meeting of Insurance & Pension, 2018

The progressive position 2, which was broadly supported at Insurance and Pension Denmark's annual meeting, was debated very thoroughly. On the agenda was the key concern that "voluntary" sharing is at risk of turning into compulsory sharing of data.

#data ethics

The picture shows CEO of the Danish Consumer Council 'Tænk', Anette Christoffersen, and CEO of PensionDenmark, Torben Möger Petersen, debating consumer protection, privacy and welfare

"To us it is important that we can all continue to get insurance on reasonable terms. And for that reason, we wish to avoid a system under which it becomes proportionally more advantageous to have a policy based on measuring of data rather than one based on general policy terms."
- Anette Christoffersen, CEO of the Danish Consumer Council 'Tænk'

Position 3 – The offensive: A good society is based on using everybody's data for the common good

In contrast to positions 1 and 2, position 3 takes a broad, societal view of the value of data. Focus is on how data – if combined, aggregated and analysed – may give us all a better quality of life. Data are seen as a valuable asset to be handled by collective (public) institutions to ensure the greatest possible usefulness for the greatest possible number of people. For this reason, Denmark must be a pioneering country, and we must use the strong level of trust in society to reap the benefits of data use.

The consequences for the many should carry greater weight than any potential risks for the few, as we do not always know what will prove to be most valuable to most people in the nearest future. With respect to welfare data, for instance (citizen data on health etc.), we ought in principle to be able to collect and store data - based on consent – with a view to being able to solve broad social problems that we have yet to learn about. With that, position 3 is placed in a basic dilemma between, on the one hand, being able to exploit the high level of trust in the Danish welfare model, while that very same trust, on the other hand, may be diminished if the industry in general collects "too much" data.

"The great majority are actually OK about sharing their health data. But I do believe that the risk for the few is given too much prominence relative to the value to the many. And in this connection tales of misuse are simply much easier to communicate than examples of the many benefits enjoyed by individual, companies and society."
– Claus Rehfeld, entrepreneur and Ph.D.

The potentially beneficial impact on society of lower health expenditure and sickness benefits is considerable if members choose to use their data in this way.

"The greatest barriers in the digital world, where we use data to create more value for everyone, are incidents of scandal involving misuse of data in large companies or governments. In such cases we all suffer, and the turnaround will then go much more slowly, or even reverse for a period."
– Sam Kondo Steffensen, program manager, DTU Business; CEO of IntraWorld Holding Intl; member of the board of directors

Commercial strengths
- Innovation and momentum at the forefront
- Data may be used to create fairer insurance products.
- Allows further minimising of affectable risks and, hence, fewer claims payments.
- Greater competitive power and export based on good, Danish public data
- Prevention and combating of fraud

Commercial weaknesses
- Focus is not primarily on the individual consumer.
- Is on the borderline with respect to social norms and consumer expectations.
- If you are part of 'something greater' the companies may lose their autonomy.

Ethical opportunities
- More special accesses or opt-out-based accesses to citizen data permit data to be used on a great scale for the benefit of many, especially in terms of prevention.
- Combating fraud, within the industry and in the public sector, is an ethical demand and is most effectively carried out using many data, historical as well as realtime.
- The companies will have better possibilities of pooling data, which is obviously in the interests of the citizens, based on opt-outs ("if you do not get back to us within 14 days, then…") and helping the less digitally prepared and/or the poorly resourced and give them better possibilities with respect to their pension, insurances and service in general.

Ethical challenges
- Not compliant with all existing ethical recommendations.
- Near-compulsory sharing of data may create mistrust and, hence, erode the foundations (the trust) for the ethical position.
- Many automatically see 'more data' as "dangerous".
- Companies assume greater moral responsibility if data sharing is opt-out-based in the 'citizens' interest'.

Position 3: Example
Jens ought to share his health data to enable the industry to find new patterns and enable more people to avoid stress and back pain. And Anne ought to share her data from her house and car to enable the industry to predict and prevent everything from flooding to traffic accidents. The choice of sharing data should not to the same degree be up to Anne and Jens. In order for companies etc. to be better at fighting disease, they should actually, for the benefit of the community, share some of the data they might not be able to see the advantage of sharing or that they would have wished to keep for themselves. This may be possible by granting of special authority to process data or opt-out-based data, which may benefit citizens who are less digitally prepared, less self-reliant and in need of extra support.

#data ethics

The picture shows CEO of PensionDanmark, Torben Möger Petersen, debating how best to safeguard the privacy and welfare of citizens with respect to data. Insurance & Pension Denmark's annual meeting, 2018

The offensive position 3 was discussed at the annual meeting 2018

The offensive ethical position, supported by a fifth of those present, was also discussed, among others by CEO of PensionDanmark, Torben Möger Petersen, and CEO of the Danish Consumer Council 'Tænk', Anette Christoffersen:

> *There are times when – if obviously in the interests of the citizen to pool data – I believe that we should practice passive consent to a much greater degree. Today, we write to people and say: "If you do not refuse, we'll be doing this with your data in 14 days…" Realising that not everyone is digitalised, we do have a challenge to assist those citizens who are not as digitally prepared as the majority. And this is where we have an obligation – by using data relating to their situation – to offer them the best possible pension or service."*
> – Torben Möger Petersen, CEO, PensionDanmark

> *I believe this to be a good idea, but it's not on everyone's agenda. Some have advanced further than others, but taking over responsibilities for some citizens unless they are in an extremely exposed situation, and not many are, to be fair – and then getting them to pull out by means of an opt-out is not a decent solution."*
> – Anette Christoffersen, CEO, the Danish Consumer Council 'Tænk'

Concern for the weakest, thus, was a recurrent and important theme, and it became clear that the industry has different answers to the same ethical problems depending on which ethical position they are talking from.

Examples of new challenges. Three case descriptions of data use and ethical implications

In the following we present three cases showing how greatly data use will create new opportunities – and at the same time raise new ethical questions. The cases have been selected to clarify the dilemmas following from ethical positions allowing greater use of data in general. The cases are from the insurtech industry, which consists of a large number of different companies, typically excelling in one or more parts of the value chain – from marketing and onboarding over underwriting and counselling to final claims handling and claims payment.

We have chosen these examples, because they represent a picture of data use with respect to insurance that to a certain extent may be deemed 'extreme' today, but not unrealistic: Because the operators exist and are solid businesses. The three cases also represent some "ethical extremes" in terms of fairness to the individual or the overall utility value. We present the cases in order to nuance the discussion and to contribute with ethical and technological perspectives.

Case 1:
Advantages and disadvantages of personalized services. The fundamental ethical themes concerning use of data are about the consequences of the new opportunities for even more accurate personalization of customers and their risk profiles and advantages and disadvantages of incentives for data sharing. Control of your own data is also an ethical theme in terms of personalisation.

Case 2:
Advantages and disadvantages of fighting fraud. The fundamental ethical themes are about problems related to supplying false information and, with that, incentives to supply inaccurate, respectively accurate, data.

Case 3:
Advantages and disadvantages of extending the value chain.
The fundamental ethical themes concern the citizens' worries about data security, and not least advantages and disadvantages of behaviour regulation based on data sharing. The case also illustrates how controlling your own data is a fundamental theme of data ethics.

Case 1: Jon Cooper on Life.io: Advantages and disadvantages of personalized services

This case focuses on the opportunities for personalization with respect to attracting customers, marketing, customer experiences and customer interaction and, not least, pricing. The case thereby also demonstrates the dilemmas of running a successful business and use of data, and raises ethical questions about who, how and why you want to insure or not insure – or at least only at a very high price. Likewise, ethical questions of solidarity and responsibility related to micro-tariffing and business models based on more and more customer data will be crystalized.

Life.io is an insurtech operator founded in Philadelphia in 2012. The operator has a total of 10 employees. Life.io is a platform designed to help insurance companies within general, health and life insurance achieve improved customer engagement through a customer-centric approach to attracting new customers. The platform offers policyholders tools to track their health, set targets and achieve rewards for improving their lifestyle. At the same time Life.io will get better data relating to the companies' customers which may subsequently be used to identify new sales and service opportunities, reduce costs and achieve greater customer loyalty.

"We focus on engaging people – building a relationship with the customer. The bi-product of that is very rich data. So first and foremost, our mission is to help individuals get more out of their insurance product. So through our platform, the carrier can engage the policy holder, set goals around their health, finances, life events and track their progress, give rewards and so on."
– Jon Cooper, Co-founder & CEO, Life.io

#data ethics

Co-founder and CEO of Life.io Jon Cooper at the annual meeting of Insurance & Pension Denmark on 15 November 2018

The business model is based on data from interactions with this online platform as well as health data, financial data, lifestyle, psychographic data such as values, interests as well as life events. Data are collected from sources like Fitbitt, Iwatch, bank accounts, medical records etc. as well as technology and AI in the form of algorithms identifying the likelihood that customers will make new or additional purchases. The machine analysis is based on large numbers of data from all customers sharing similarities. Thus, Life. io is an example of how marketing models from tech giants (such as Amazon) are copied by the insurance and pensions industry.

"We help carriers to do the same thing as Netflix and Amazon are doing. When they are recommending a product, it's not based on my previous behaviour but on other people similar to me and what they do. And it's important that carriers are equipped to do the same thing because it's not such an insulated market anymore. Amazon is moving into the insurance industry and data is a key asset in the insurance industry."
– Jon Cooper, Co-founder & CEO, Life.io

The business model is very much based on the customer relationship and the customer's willingness to share this with the platform. And when sensitive data are at stake, the task will be to explain to the customer why he or she should share the data and how the individual will benefit from sharing them.

"At the end of the day, we're gathering a lot of data to benefit customers and carriers. But a lot of this data is sensitive health data and financial data – and we have to focus heavily on the consumer design element and value exchange in order to make this whole thing work."
– Jon Cooper, Co-founder & CEO, Life.io

This naturally raises the question of transactions and exchange of data for, say, financial value, as incentives for transactions that may have a socially imbalanced effect, because those with smaller incomes will feel a greater incentive to supply data in return for money than those with higher incomes. Financial incentives may also affect the judgment of the individual, prompting him or her to make decisions that in the long term will prove irrational, although rational in the short term. On the other hand, data may also be considered an asset owned by all. And for this reason, incentives for data-sharing will not necessarily change the inequality that already exists.

"I think GDPR is great. Consumers need to understand how their data is being used. But I don't think it will change behaviour. As a consumer, the cheapest form of currency that I can use is my data and if you'll give me something in exchange of that 'go ahead'. And I think it's important to have a robust regulatory landscape in place so that this can't be misused."
– Jon Cooper, Co-founder & CEO, Life.io

How do we relate to the question of fairness and solidarity?

The case involving Life.io illustrates the potential of data use and personalization of the customer segment and at the same time raises the question of how far down the personalization trail we can and should go with respect to insurance, and how two fundamental principles of insurance – fairness and solidarity – are brought into sharper focus by the new uses of data. Because, to a certain extent, data may counteract discrimination, which is an effect of 'personalization' and constitutes the basic theme of data ethics in this case.

Personalization is taking things one step further than segmentation. And further personalization may wreck the statistical models that place people in specific risk segments. More data points may determine whether you actually fit into a specific segment or, perhaps, would be better placed in another. Increased use of data, thus, may to a very considerable extent provide very accurate and, with that, fairer risk assessments and more exact categories and fixing of premiums, albeit within the traditional insurance paradigm involving risk pools. And the latter also carries a potentially stabilizing effect with respect to the very large datasets which, to be fair, are still not entirely accurate[6].

It may be argued that as soon as you choose to tariff with respect to specific data points and priceset based on individual data, you will, as an actuary, be responsible for doing it as accurately as possible. If more data points may contribute to deciding whether a policyholder should pay less, is it then fair to insist that she should pay more, because there is a certain limit to how much data you can collect? And, taking the opposite view: If more data show that the policyholder actually is let off more cheaply than he 'objectively' deserves, is it then fair to the other policyholders in the pool that they must pay for his risk?

Using many data, it will obviously be possible, theoretically, to create more individualized insurance based on insurers knowing so much about the policyholder that his or her risk is completely accurately calculated.

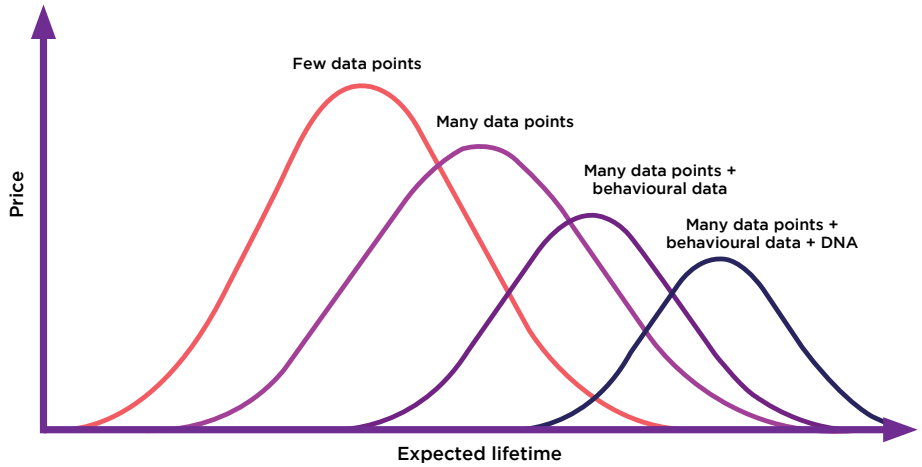


Figure 7 shows the normal distribution within insurance pools that become more and more accurately calculated the further we proceed down the x-axis (expected lifetime). The number of people who live to a great age, but unfairly pay the same as those living shorter and more risky lives, will be reduced the more data we use. The number of unjust relations between policyholders in the pools will, so to speak, become smaller the more data we use when underwriting. (Note: Today it is not allowed to use DNA data in insurance, nor does the industry wish to use DNA in insurance or pension cases. This element is included in the figure to illustrate the point about the progression from few "superficial" data points to more and more intrusive data points).

"If you take someone who is in his forties, has diabetes and hypertension, he'll pay the highest premium based on mortality tables. But if you take it to the next layer and really analyse that data and combine it with lifestyle data, there is a group in there that should be super-preferred. They have the same mortality risk and life expectation as the usual super-preferred risks because they manage their diabetes, take care of their health, take their medicine etc. That level of precision doesn't exist today with the way insurers manage risk – but more data will help insurers make much more personalized insurance. It can never be individualized because that destroys the whole purpose of pooling risk but breaking it down further than we do today makes a lot of sense in this scenario."
– Jon Cooper, Co-founder & CEO, Life.io

The individualistic insurance model does not pool risk, rather, it pricesets risk accurately. In that scenario the solidarity principle of insurance will be challenged. Many associate the solidarity principle with the systematic redistribution taking place through the tax system and the welfare society that we have created in Denmark. However, if the industry did not already use data to personalize the price of insurance, an ethical problem would emerge as to whether it would be fair to have the teacher with three kids pay for the person who has chosen to dedicate his life to martial arts. It would also raise questions about moral hazard if individuals can choose to do senseless things liking building a house right on the shoreline. And if we abandon solidarity in insurance as the redistribution that takes place from those who do not have accidents in favour of redistribution to those who do, then personalization and solidarity will not appear to be mutually exclusive.

Personalized services will naturally become more nuanced with respect to data sensitivity, e.g. damage to property and personal injury

It is possible to imagine a world in which many will share data that will become more and more accessible because of the growth of IoT, for instance, while others will refrain from doing so. In that case we shall see an insurance market much like the present with much finer gradations between high and low risk groups. Some will have a greater incentive to share data than others, and, therefore, we are likely to see this scenario unfolding primarily where considerable cost savings may be reaped. Within damage to property at present, it would be old houses (with old water pipes) and young car drivers.

> *"Today, there are people who accept paying a higher premium in exchange for having to share less data. Because they know they're high risk or because having to share data is perceived as inconvenient. And then there are people who are willing to share more data because they are curious and want to have that level of precision. I think this trend will continue but with the spectrum getting broader, enabling me to eventually go down to the epigenetic level perhaps and find the 'super-duper preferred risk group' consisting of people who are actually willing to share that kind of data. And as you go further upstream and people are willing to share less data, they're going to be pooled in larger higher risk groups. So, it will be the same market as exists today, but the number of tiers in there will just be far greater if you ask me."*
> – Jon Cooper, Co-founder & CEO, Life.io

Already today we are seeing that increased data collection through IoT etc. and sensors in the form of tariffing and pricing being used within the field of property damage, where data are not personally identifiable and therefore less sensitive. So, this sort of data collection with respect to fire and water damage (and especially prevention of such damage), which represents a considerable share of costs, will become much more accessible. On the other hand, dynamic behaviour data, such as personal behaviour data – in contrast to statistical data like age, address, education etc. – will result in a type of market differentiation where low-risk groups will share more data and be very accurately tariffed, whereas those with higher risks will share fewer data and end up in larger pools. Here "controlling your personal data", and the possibility of sharing more of your personal data with insurers or pension operators – or not sharing more data - will play a key role for the development of the market. As a result, controlling your personal data will become an important ethical theme with respect to data for risk assessment and more personalized price and services.

To exemplify this, let us look at a theoretical example involving the policyholders Anne and Jens. Anne has a long-cycle education and lives quite sensibly in contrast to Jens, who suffers from certain disabilities. Anne will have a greater incentive to share data than Jens, and because of the free choice, there is a risk that her premium will be more accurately calculated because she is willing to share more data. The insurer will be better able to calculate and understand Anne's risk, which is low, and therefore she will be more accurately placed at the low end of the risk scale, also reflecting the price – illustrated as price bands – that respectively Anne and Jens would have to pay for their policies. And because Jens shares fewer data and is not forced to share the same data as Anne voluntarily shares, he will end up in a large high-risk pool in which there will be more people with a relatively low risk who – in figure 7 above - in principle pay unjustly for the high-risk individuals paying the same as them, even though they carry a higher risk. Both Anne and Jens have sensors in their house, partly because they do not record sensitive, personal data, partly because they both benefit from being able to prevent damage. Anne's house is closer to the water, and the risk of water in her basement is greater than for Jens, who lives further inland. In this scenario, the premium will be equally accurately calculated for both houses, and we do know why Anne must pay more than Jens.

PERSONALIZED SERVICES WILL NATURALLY BECOME MORE NUANCED
WITH RESPECT TO DATA SENSITIVITY, E.G. DAMAGE TO PROPERTY AND PERSONAL INJURY

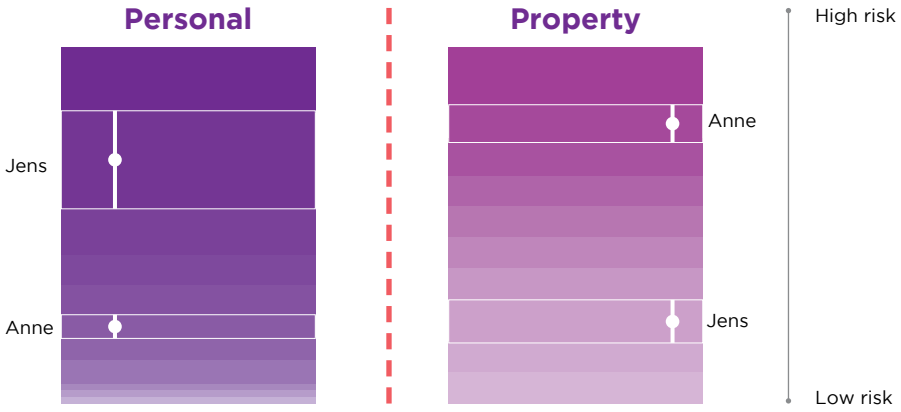


Figure 8 describes two theoretical scenarios with ethical implications. In both the left and the right scenario increased use of data has created a larger difference between two different policyholders, exemplified by 'Anne' and 'Jens'. In principle an A-team and a B-team might emerge in both places, but it would be more sensitive in the 'personal' scenario on the left. In both cases it would often be in the interests of both the policyholder and the insurer to motivate the greatest number of those on the B-team to improve their risk profile with a view to getting a cheaper policy. The horizontal lines in both columns illustrate simultaneously risk pools and price bands, where everyone within a given risk pool pays the same, regardless of whether they are at the high or the low end of the pool.

Data, in other words, may bring about a personalization that will change the segmentations/ profiling we see today, and, everything else being equal, increase differentiation within the field of personal injury and facilitate the emergence of and A- and a B-team. And this raises ethical questions with respect to what solidarity-based solutions the industry (in collaboration with the welfare society) may develop for groups that, based on multiple data, appear to be difficult to insure.

> *When it comes to micro-tariffing, there are customers who will see enormously high premiums, which is very likely to have an imbalanced social effect. This is where the government may help, but that will have consequences: We will get a marginalized group, a stigmatized group and not least a group that will get relatively poorer solutions than those serviced by insurance operators, because the government's services usually are relatively poorer."*
> ."- Thomas Ploug, professor at Aalborg University, Ph.D. and former member of the Danish Council on Ethics

Among companies within the industry, experts of ethics and use of data in the international InsurTech industry, there is broad agreement that increased personalization is beneficial, but a line is to be drawn at individual risk assessment. However, there is a lack of agreement about what solutions should be offered by the industry, society or state to people of very high risk.7 This may be a matter of industry-wide solutions, government solutions, such as mandatory joint schemes like flooding contribution, natural disaster pools or semi-voluntary communities, which characterize the Danish model, such as solidarity-based communities like the group-life insurances that are often connected with labour-market pensions.

Is data sharing based on free choice an illusion?

Free choice is certainly an important ingredient when it comes to using data for risk assessment and pricing of individuals. Informed consent is key to the insurance and pensions industry, but it presupposes transparency about what the individual agrees to or not. And if the alternative is sufficiently poor, the free choice of sharing will be an illusion. For this reason, the alternative to sharing of more sensitive personal data must not be discriminating or jeopardise the interests of the individual.

In this way the case also illustrates how the many new opportunities and challenges posed by data require of the industry, to a much higher degree than so far, that it explains to the surrounding world across stakeholders what ethically value-creating benefits will be available, and a willingness to discuss the consequences that data and technology may help relieve. Use of more data for pricing of risks may result in two scenarios that are not mutually exclusive:

- First of all, more data for the purpose of fairer pricing may result in more people having to pay less, because the worst risks will have become more narrowly segmented and further isolated. If such high-risk groups are able to change their risks by means of initiatives to regulate behaviour, this may create value for both themselves and society as a whole (more about this under case 3). We are talking about an absolute reduction of prices, because aggregated risks have become lower.

- The other scenario is that there will be a small group who are unable to change behaviour or, for example, live on bog land where the risk of water in their living room is considerable. The concrete problem exists in the form of 'red houses' that are currently becoming uninsurable as water damage from flooding systematically reoccurs every year. For this segment, knowledge about the location of these risk groups, and who they are, is valuable. In that case, perhaps, other social institutions may need to develop and offer solutions to be undertaken by the community in one form or another. For instance, by having the local authorities purchase the red houses and pull down those that are most exposed, followed by draining of the area in order to prevent water damage to the remaining houses.

> *"What I'm telling regulators is that if someone is able to isolate the worst risks, that is a good thing. Because if it is something that can be changed – like driving behaviour or lifestyle etc. – insurers will try and create specific products for these bad risk people. It sort of gives the sector incentive to change behaviour that can be changed. And then there are things that can't be changed nor controlled by the customers. And here I think we will have very small clusters that society then can decide what to do with, and e.g. give the 0,5% of people who are inherently bad drivers the money to take a cab instead."*
> - Matteo Carbone, Director of the IoT Insurance Observatory (previously Connected Insurance Observatory), Global InsurTech Thought Leader & Investor

Personalization from the perspectives of the three ethical positions

In position 1 many will believe that the consequence of using data is too great with respect to the few potentially non-insurable, and this is not counterbalanced by the fairness-benefits to the many. Nor is there willingness to accept the potential discrimination inherent in the philosophy "share data or get a poorer product". In both positions 2 and 3, on the other hand, there is agreement that more data creates great advantages to the individual and the community. In position 2 possibilities will be created for the individual to share as many data as he or she wants in order to be as accurately assessed as possible. This is fair to the individual but presupposes a real alternative to ensure that it is a choice to be made freely. In position 3, on the other hand, many will attempt to get authority to process information that will allow more data about everyone in order to find optimal solutions for the majority. Those who are in position 3, then, will justify massive use of data to isolate the very worst risk groups, primarily to ensure that many will need to pay far less and secondly get the opportunity to develop optimal solidarity-based solutions to those groups that are extremely expensive to ensure. This may be through more intelligent town planning, through greater knowledge about building sites, water tables, climate change etc.

Summing up: Greatest opportunities and challenges of personalization

- The Life case illustrates the great potential and challenges linked to use of more data from the perspective of the fundamental ethical theme of 'personalization' of risk assessment and pricing. Increased personalization may lead to more accurate and fair risk assessment and pricing but also to identification/isolation of the weakest groups, which is a key ethical dilemma linked to personalization.

- In Denmark, it must be said, the real cost reduction of sharing more data is minimal. Appreciable reductions are only to be expected with respect to old houses and young car drivers.

- The case illustrates how, especially with regard to personal injury, ethical dilemmas of greater use of data will emerge in terms of risk assessment. But in Denmark, especially for health insurance, this problem is not quite as important as in other countries as we have decided that everyone must pay the same price for healthcare regardless of individual risks.

- The case moreover illustrates how the traditional principle of solidarity, understood as systematic redistribution, is irreconcilable with personalization, which is linked to the ethics around fairness to the individual and the insurance community. Fewer data for risk assessment will lead to greater injustice to individuals who are priced too highly or to others if they are priced too low.

- The case, then, also illustrates the value-creation of using data to break down stigmatising and unjust segmentation of groups based on few data points.

- The case illustrates that a high degree of personalization and solidarity, understood as unsystematic redistribution from non-injured to the unfortunate ones may function concurrently and without conflict.

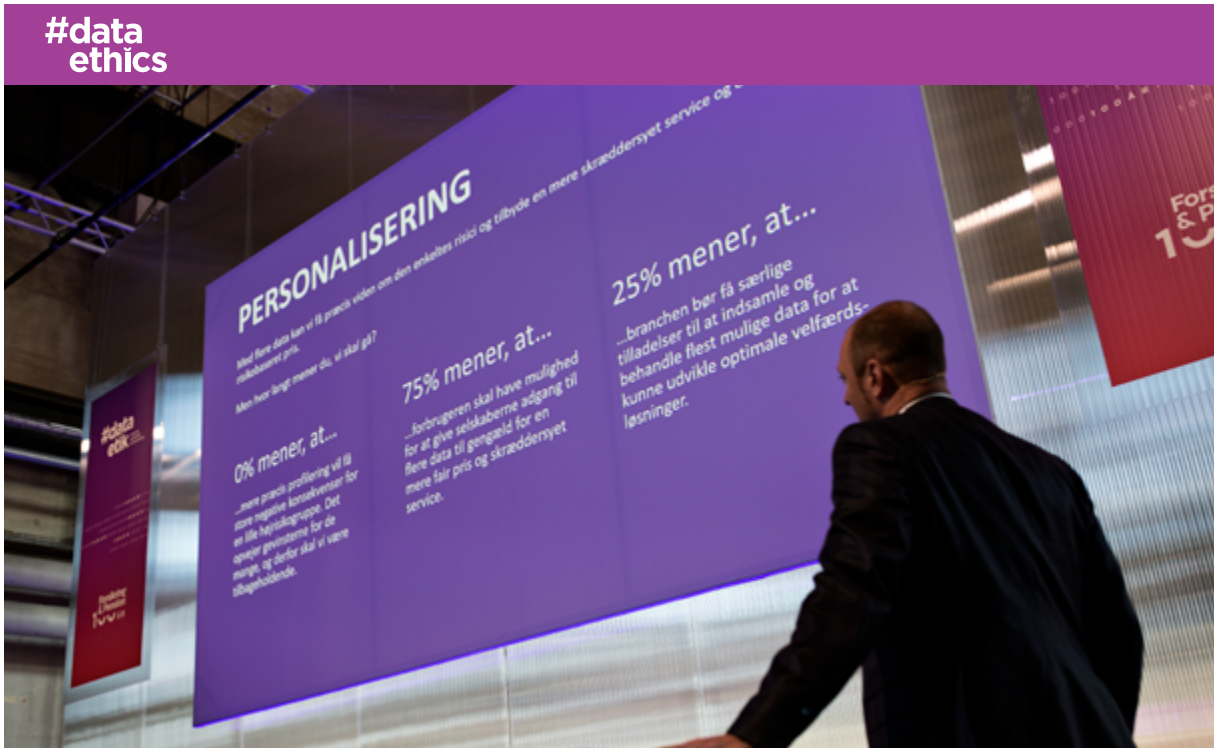
- The case illustrates the ethical problems raised in terms of the theme of 'incentives' to data sharing in return for lower prices/reductions etc. In this regard there is a risk that such transactions will impact in a socially imbalanced way without necessarily increasing inequality but rather confirming existing inequality in society. In addition, financial incentives will mean that further data sharing will take place within areas where the benefits of, especially, dynamic sensor data will be appreciable.

- The case also points to how such incentive to data sharing may change pools within the existing insurance market to the effect that, especially within personal and behavioural data, differentiation may emerge from high to low risk groups resulting in several small pools paying less, while fewer large, high-risk groups will pay more. This differentiation will take place within the field of personal injury but probably to a smaller extent than within the field of property damage. The relevant ethical discussions will be limited to the field of personal injury, involving A and B teams.

- By the same token, the case illustrates that transparency and personal choice play a key role for the development of the market and the consequences for the weakest and most risky groups. In this connection, controlling your own data becomes an important ethical theme and a precondition for a potential market development towards more and more accurately calculated groups at the bottom of the risk scale and larger groups at the top. And, indeed, this is how the market has developed in Denmark over the last many years.

- The case also gives rise to reflection about the problem of the 'illusion of voluntariness', where the customer either shares data with consent or receives a very poor alternative. This does not reflect a genuine free choice, which is a key element if the industry is to justify, ethically, the use of more data for better risk assessment.

- The case opens up opportunities for insurance products becoming accessible to far more groups than today if policyholders are motivated to improve their risks and become 'insurable'. The great potential, ethical challenge, however, emerges in this very process as there is a potential risk of non-insurable individuals or groups (e.g. 'red houses') emerging. Groups that we as a society may owe an ethical obligation to offer a solution, perhaps in terms of a max-band that everyone must be insured within in a specific country or in the entire EU, or that we jointly, over taxes, finance the purchase of exposed houses and offer rehousing of the occupants.



The picture shows CEO of Topdanmark, Peter Hermann, on the main stage. Previously a number of the participants at the annual meeting had specifically discussed the theme of personalization, and, as things stood, 0% choose to vote for that position, while respectively 75% and 25% choose the progressive and the offensive positions.

Personalization debated at the annual meeting of Insurance & Pension Denmark, 2018

At Insurance & Pension Denmark's annual meeting on November 15, 2018, personalization was discussed and debated. CEO of Topdanmark, Peter Herman, commented on the debate:

> *I believe – as is also reflected in the vote at this annual meeting – that we should focus more on using the data we already have. But there were also some relevant questions as to how we as an industry ensure some form of fairness, and which data we then will use."*
> – Peter Hermann, CEO, Topdanmark

The key dilemma of solidarity versus fairness was also discussed, including how to interpret the concept of solidarity:

> *With respect to the discussion about solidarity, I do believe that it is important to say that the greatest equalization takes place between those who report no claims and those who do. That is the first point. The other is to say that when we speak of solidarity, it is especially with regard to the possibly ruinous cases that we need to speak of this."*
> - Peter Hermann, CEO, Topdanmark

Subsequently, CEO of PFA, Allan Polack, touched on the potentially self-defeating element of massive use of data for risk assessment etc.:

> *Using more data, we might end up with segments of one. And if that happens, we will have disrupted ourselves, because that eliminates the collective element of insurance altogether. So, how far are we to go on and say: "I know all about you, so it's all very fair. Only thing is that you have to pay for your own claims."*
> – Allan Polack, CEO, PFA Pension

CEO of Topdanmark, Peter Hermann, also reflected on the industry's ethical task and the significance of competition:

"As for some of the other elements of insurance, they seem to me to be working like some of the other financial services, and I do not believe it is the industry's job to attempt to equalize all socio-economic differences in our society. If so, I believe we would have to use vast numbers of data to create greater competition, and that might make us even more granulated, so that all differences are really erased."
– Peter Hermann, CEO, Topdanmark

The question about a realistic alternative to products against data sharing was also debated later in the day during a panel debate, during which fears were expressed that voluntary data-sharing might develop into an indirect requirement in order to obtain a fair insurance premium'

"We may choose to make data available via all sorts of exciting apps that are continually being developed. But if it gradually becomes mandatory that you must allow access via consent, it turns into some kind of pseudo-consent, because as citizens will indirectly be forced to supply those data about ourselves if are to have any hope of getting affordable insurance."
– Sophie Løhde, Minister for Public Sector Innovation and member of the Danish parliament

Case 2: Advantages and disadvantages of using data to combat insurance fraud

Insurance fraud is a general problem of the insurance industry in all countries. Insurance fraud means that, every year, all policyholders must pay higher premiums than strictly necessary. As not every instance of fraud is discovered, it may be difficult to state the exact scale of insurance fraud in Denmark. In a report from Insurance & Pension Denmark, based on data from those insurance and pension operators that do carry out fraud surveys, it appears that in 2017, 3943 cases of insurance fraud amounting to a total of DKK 594 million were reported. Out of this amount, fraud on damage to property (car, travel, home contents and building insurance) accounted for DKK 208 million distributed on 3531 cases, whereas fraud on personal injury (work-related injury, accident, third-party vehicle and travel insurance as well as disability insurance linked to pension schemes) accounted for DKK 386 million distributed on 412 cases. Based on the assumption that the other insurers of the industry take similar measures with regard to fraud, and discover the same extent of insurance fraud, the figure for the entire industry indicates insurance fraud worth DKK 976 million distributed on 5262 cases in 2017. International surveys indicate that insurance fraud accounts for 10% of indemnity payments internationally. Using this figure for Denmark, where insurers paid indemnities amounting to DKK 43.3 bn, insurance fraud runs into DKK 4 bn, which translates into DKK 1500 of extra premium payments per household in Denmark[8].

"Many of the things we do to protect consumers are out of misunderstood kindness. It is problematic that every Dane must pay up to DKK 1500 more, because some people are unable to behave properly. We witness the same sort of thing in terms of social fraud, where certain individuals cheat the community. I find it difficult to understand why we don't have much greater focus on fraud."
– Henrik Bundgaard, Claims Director, CODAN

Combating insurance fraud has long been a matter of investigating property claims. When it comes to life, the industry has traditionally been more reluctant to identify and investigate suspicious cases, partly because of the duty to inform the citizen that he or she has been under observation, and partly because of the great risk of negative stories in the press.

The same is true of the different foreign, common claims registers, which all primarily contain information related to property claims. In Germany, the industry has now started discussing a similar model for health, where fraud accounts for around 8.5% of claims payments. Recently the Health Insurance Counter Fraud Group (HICFG) in the UK has also started looking at how to combat fraud within health insurance by means of a common data base.9 This may indicate that norms are sliding towards acceptance of using certain tools of data collection, storage and sharing to prevent fraud on health insurance. An area, incidentally, where, typically, very large sums are being defrauded in each individual case.

For many, anti-fraud measures are, ethically speaking, a matter of surveillance. And in the cases brought to public knowledge via the media, it has often been a matter of a very thorough investigation by the insurer or pension operator to decide whether a particular individual has been entitled to indemnity payment. The truth is that a large number of choices are made up until the moment when an investigation is launched. This means that, ethically speaking, it is not a matter of mass surveillance – i.e. lack of control of your personal data used in the administration of a policyholder's claim – because pattern recognition and rules are launching collection of gradually more and more data – like a decision tree – if a claim shows signs of possible fraud. On the other hand, some Danish companies are also experiencing customers who complain about the lack of surveillance and control if they merely have to answer a limited number of questions in order to get their indemnity payment. Such customers feel a sense of insecurity because if "it is so easy for me", it must be equally easy for the fraudster. Therefore, the balance is difficult to achieve, when experienced 'surveillance' can be perceived as being both too much and too little.

The surveillance-related, ethical problem of using data to combat fraud, then, is not a matter of keeping many under surveillance in order to catch the few – even if a lot of people believe this (for good or bad) -it is rather a problem that emerges if someone is unjustly subjected to intensive control and surveillance, i.e. the false-positives who have done nothing wrong but are nevertheless being thoroughly investigated.

In this publication use of data for identification of potential insurance fraud is not generally seen as a question of surveillance but rather as one of solidarity with the individual and the community and, especially, as an incentive to not giving wrong information at the expense of others.

Insurance fraud in the digital world

Insurance fraud may be identified by means of various systems that the insurers may individually acquire. More datasets, combination of data and pattern recognition are key to identifying possible fraudsters, but they are not absolutely necessary. Internal claims data, police data, claims assessors' reports and bills/photos may be cross-referenced with external sources such as geolocation, weather data, operator information and telematics. Actually, only legislation and ethics bar the way to how many data the industry is allowed to and wants to use to identify possible fraudsters. AI, machine learning and combining data may significantly increase effectiveness and identification of possible fraudsters as well as reduce the number of false-positives exposed to unnecessary control who represent the ethical problem of baseless surveillance.

> *"We see that the risk of fraud increases as claims administration is increasingly being carried out digitally with many people typing in their information at home. The boundaries for what is OK to report with regard to incorrect information, unfortunately, appear to be changing because processes have become more digital and the human contact points between policyholder and claims administrator have been reduced."*
> – Brian Wahl Olsen, Director of Claims, Alm. Brand

In a more digitalised world, claims administration, too, will become more and more digital. There are indications that the scale of insurance fraud will increase, once the customer no longer needs to call up the case administrator but may simply enter all the information on the computer at home. 11 This makes new demands on the insurers' methods of combating fraud. Not only for identification of possible fraud cases, but also with respect to preventing fraud and motivating customers not to give incorrect information at the expense of all the rest of us.

"Combating fraud is about digital business development. If more people give false information when reporting a claim, it means that we shall have to turn up our fraud-detection systems, combine more data in realtime and work with prevention and attitude-changing measures in order to withstand the pressure. And then the actuaries, hopefully, will not need to change their pricing models, which, again, will affect all the other customers who will have to pay more for their systematic risks."
– Brian Egested, head of dept. and member of the board of directors, Alm. Brand

The trend towards more fraud may in principle affect the honest policyholders more than the DKK 1500 a year of extra premium they pay because of fraud due to skewing of the insurance pools. Calculations may in principle have to be changed to reflect the larger number of claims within the pools that the fraudulent data wrongly contribute to adding. Therefore, combating insurance fraud is, ethically seen, also a question of minimising the quantity of false data – i.e. fraud – so that the honest policyholders' risk is not calculated wrongly due to the unethical behaviour of fraudsters. This may be done partly by turning up the volume of data, combining more data across sources and using AI to discover patterns between many data points, partly by turning up prevention and trying to remove people's incentive to give false information when reporting a claim.

"Clearly, there is room for improvement in terms of using more data points and better aggregation of data. And we are constantly becoming more knowledgeable about the data to which it would be relevant to add value. We need the data that provide actual value and not merely to use all available data and end up with a large number of false-positives, having inconvenienced ordinary, honest policyholders in that process."
– Brian Wahl Olsen, Director of Claims, Alm. Brand

Here we encounter a difficult dilemma between utility value, respect for the individual and relevance of data collection. If everyone must be exposed to increasing collection, registration and sharing of data in order for the few fraudsters to be discovered – e.g. by answering all 15 additional questions on the claim advice – we may end up casting a suspicion which, for the majority, is entirely unnecessary and unjustified. And policyholders will become frustrated and their relations with the insurer will suffer. And considering that policyholders expect claims to be dealt with swiftly, followed by prompt payment of indemnity, it might be an easy solution to introduce a trifle limit for when it appears relevant to take measures against a potential fraudster. But why is it ethically justifiable for the individual to pay for the fraud of others which falls below any particular trifle limit? Moreover, the threshold limit may also be strategically exploited by the most cunning policyholders. Combating fraud is ethically a difficult balance to strike between hard ethical choices, concerns for both usefulness and the individual (using both a few and many data), but it is also a problem that may be alleviated through technology.

Can more data used intelligently with AI improve combating of fraud?

By means of digitalization, data from such sources as BiQ, DMI (weather), police data, reports of claims assessors etc. may be combined in a databank. The machines are able to see patterns that appear suspicious or resemble other cases of fraud. Suspicious cases are marked, and the claim administrator will be informed at the point of receiving a call from the policyholder whether something suspicious is afoot. The claim administrator will then ask the 15 clarifying questions if relevant. The honest customers' claims, however, will be dealt with easily and painlessly without any hint of suspicion or need for control questions. The technology, in a manner of speaking, alleviates the problem that insurers must be able to check on us all. It enables us to use data in a way that facilitates targeted combating of fraud to ensure that as few honest policyholders as possible are inconvenienced. Let's take a closer look at what the operator Shift Technology is doing.

Shift Technology is an InsurTech operator based in Paris. The operator was founded in 2014 and has a total of 90 employees. Shift Technology offers insurers advanced anti-fraud systems. Shift employs a large number of 'data scientists' who teach machines to discover patterns indicating fraud. These scientists are placed with the insurers and talk to experts of claims and fraud and pass on the knowledge they acquire from the experts to the machines.

#data ethics

Director of Shift Technology Bo Søvsø Nielsen at the annual meeting of Insurance & Pension Denmark on 15 November, 2018

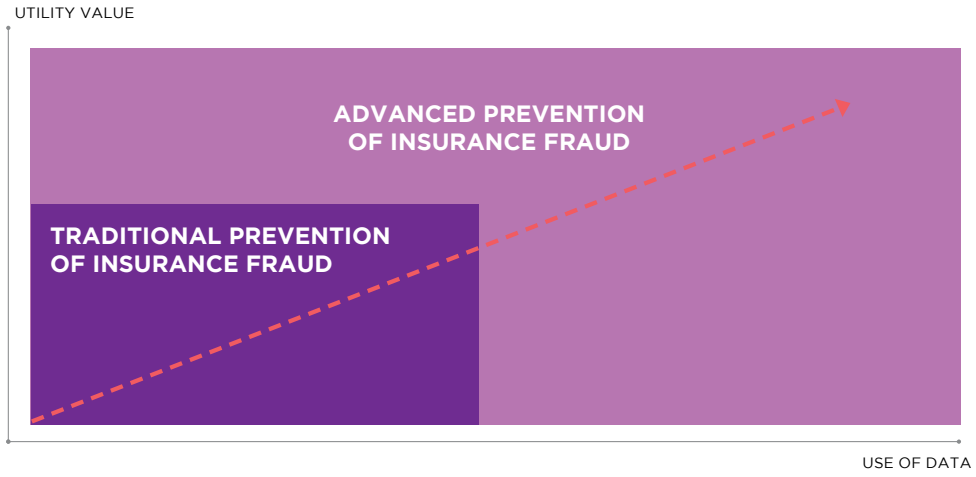
"We identify suspicious claims by comparing data points and their links. We have developed the 'recipes' of data points and indicators behind patterns of fraud. You don't really need a lot of data points, because using statistics, algorithms and machine learning you can teach a system to see patterns of fraud by using historical data. But in order to raise the quality of alarms and reduce the number of false-positives, we recommend using many data sources."
– Bo Søvsø Nielsen, Director, Shift Technology

Shift Technology is an example of data sources being collected in realtime, with algorithms setting off action-oriented alerts based on statistical probabilities from use of specific words, order of words and patterns etc. These data belong to the insurance companies, which have either bought or have legal access to them. Shift are not data administrators but data analysts.

In the long term, reporting and administration of claims may be far more automatic and involve immediate payment of indemnity. So, in this regard, we will see fraud investigation becoming much more intertwined with claims administration. The questions asked when a claim is made will be reduced to two or three combined with a large number of already accessible data and automatic image recognition. If the machines, already at this point, are able to detect suspicious patterns, additional questions will be asked about specifically those areas. This will be effected within both car, travel, house and health insurance.

Shift Technology represents a paradigm for combating fraud, and the utility value is represented in the form of identification of fraud cases, the number of false-positives and targeting of control questions and further data collection increasing concurrently with the number of aggregated data points.

Figure 9 shows modern claims administration and combating of fraud. Different data are entered into the machine, which then analyses the data and subsequently alerts the claim administrator if there is reason to be suspicious.



Figur 10 basically describes two paradigms of how to combat fraud. Traditional combating of fraud is based on specific threshold values and relatively few data points in combination with simple rules to determine when a claim is suspicious. Modern combating of fraud, as exemplified by Shift Technology, is based on far more data points and complex patterns that, in combination, may indicate whether a claim is suspicious. More and more data create more and more intelligent and effective combating of fraud.

Is a common claims register possible in Denmark?

A consequence of the technological possibilities, however, may be that some insurance fraudsters shop around among insurers, changing to companies that do not employ technology facilitating fraud detection. The Danish insurance industry does not have access to data on the claims history of property, such as claims involving a car or a house. Many other countries have established common claims registers to avoid fraudsters merely moving on to other companies. In France there is the ALFA, in Germany the HIS database, and Finland, Hong Kong and Spain also have common claims registers for the same purposes. Our Nordic neighbours, Sweden and Norway, have respectively the *Gemensamma Skadeanmälningsregistret (GSR) and Forsikringsselskapenes Sentrale Skaderegister* (FOSS)

There are different parameters to bring into action to reduce the incentive to defraud. In all likelihood, awareness of a common claims register will affect the motivation to defraud. The prospect of severe punishment will have the same effect. Knowledge of the insurers' anti-fraud systems and threshold values may also, as described, have a certain effect. And finally, there is ethical awareness in the shape of the claim advice. The ethical imperative is here to create an incentive for the customer to reflect ethically when reporting a claim.

Incentives seen from the three positions

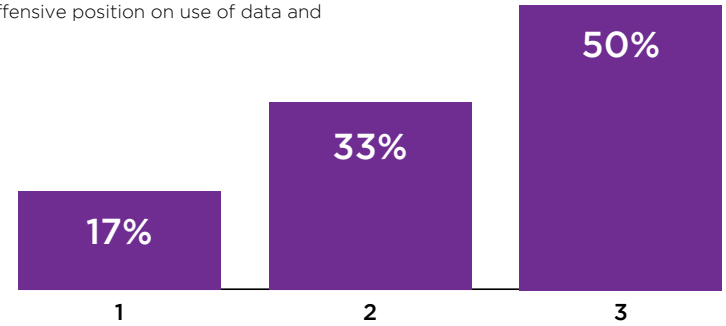
In position 1 you will be deeply sceptical of incentives to use data for combating fraud. In this position you will talk of surveillance. You will see it as an expression of suspicion being cast on the many in order to change the behaviour of the few - who, after all, often only exaggerate mildly when reporting a claim (soft fraud). In position 2 you will not accept the logic that insurers should accept or disregard a certain amount of fraud, because the costs to the individual, honest citizen should be minimised as much as possible and cannot be likened to concerns about the contract of trust between consumers and insurers. You will therefore be ready to use more relevant data points and automatic combination of data to avoid inconveniencing the individual unnecessarily in the name of common utility. Incentives to give true information are legitimate, but care should be taken not to appear patronizing or exerting mind control. In position 3, however, you will be turning up the volume of data to a maximum for the good of the community. Even if the marginal utility value of the next data point is lower than for the previous one. Moreover, in position 3 you will be in favour of registering claims data in a common register, and you see insurers as almost morally obliged to share data with public authorities in order to contribute to combating social fraud. Incentives and attitude-changing initiatives are completely legitimate, and influencing the way people think is always ethically justifiable, provided it is for a good cause.

Summary: Greatest dilemmas of combating fraud

- The Shift case illustrates the dilemma of the utility value of using more data to identify possible instances of fraud versus unnecessary and unjustified control of the many honest customers in order to capture the few fraudsters.
- The case also illustrates the dilemma between concern for the consumer in terms of the quantity of data collected and registered versus the amount of fraud you are willing to accept and that, of course, the honest policyholder must help pay for.
- More data create greater utility value in terms of more accurate identification of fraudsters and fewer false-positives. But it is not absolutely necessary to have many data sources to identify possible fraudsters. So, the question is how to find the right balance in ethical terms.
- The case illustrates that more data points and different data sources may advantageously be combined to achieve even better detection of fraud without inconveniencing honest policyholders unnecessarily. More data and AI, it appears, can potentially solve the conflict between looking after the policyholders' money or privacy, or doing both by means of intelligent pattern recognition, so that data need only be collected when there is good reason for suspicion.
- The case illustrates that new data uses, especially with regard to identification of potential fraudsters, will be of great importance to claims administration and detection of fraud which, to some extent, will become fused and operate automatically.
- The case illustrates that with increasing digitalisation of claims reporting, there will be an increasing need to counter fraud through systems and, preventively, through incentives to customers taking an ethical stand with respect to the claim advice.
- Finally, the case illustrates that incentives to supply false or true data when reporting a claim constitute an important ethical dilemma.

#data ethics

Figure 11 shows the distribution of votes on, respectively, the critical, progressive or offensive position on use of data and combating of fraud.



Combating fraud debated at the annual meeting of Insurance & Pension Denmark 2018

Combating fraud was debated and discussed at the annual meeting of Insurance & Pension Denmark on 15 November, 2018. A number of the participants had debated the theme of combating fraud and the extent to which the industry should go in collecting data to combat fraud. As it appears from figure 11, 50% preferred the offensive approach, involving large-scale use of data and sharing among companies and the public sector in order to prevent social fraud, too.

#data ethics

The picture shows group CEO of Codan, Vivian Lund, on the stage commenting on the ethics of combating fraud.

The reason why the offensive position 3 weighed more heavily here than in the other polls may be the subject and the dilemma between concern for the individual and for the collective.

"The scale of fraud is huge: You know, four billion a year is just what the insurers report; on top of that we have social fraud. It is a shockingly large figure in reality. And I do believe that the result of the voting is driven by the balance we must achieve between concern for the individual and for the collective. And in this instance, the individual is of course the fraudster. And there isn't the same feeling that this is an individual we need to protect".
– Vivian Lund, Group CEO, Codan

The debate about surveillance was also concerned with the question of how far we are willing to go to catch fraudsters – or whether technology may render superfluous this discussion and fear that many share:

"Often, we worry about those who, for a time, come under suspicion or whom we need to clear or confirm as fraudsters. In these cases, it is quite legitimate to worry about the quantity of data used and how close you get to the individual. And I believe that is what the 17% feel. And in this connection it was incredibly interesting, earlier today, to hear Bo (Bo Søvsø Nielsen, Director, Shift Technology), when he had the floor, say that with the right data he would be able to reduce the share of those wrongly suspected of fraud to somewhere between 10-25%, given a hit rate between 75% and 90%"
– Vivian Lund, Group CEO, Codan

Case 3 Luca Schnettler on HealthyHealth: advantages and disadvantages of prevention

With the many new data and analytical tools, insurers and pension operators get the possibility of working with predictive analytics and preventive counselling with respect to risks and life insurance rather than reactive compensation. And in this way the value chain and the portfolio of services are increased. The purpose of the third case is to illustrate the possibilities for creating a health system in which interaction of operators, use of data and preventive efforts strengthen the welfare society and the welfare of the individual. The insurance and pensions industry constitutes an important part of the infrastructure of the welfare society and health system. But today companies are subject to restrictions that rein in insurance activities, and as a result insurance companies cannot go very far into other related value chains in, say, the health system. However, for the present purpose we shall put brackets around such regulations in order to investigate opportunities and challenges of extending the value chain. HealthyHealth is such an example. This operator always offers risk probabilities for up to 800 diseases, thereby, they claim, reducing claims payments by 4-9%. For pensions the same preventive philosophy is applied: HealthyHealth helps individuals budget their pension funds, estimate health expenditure on medication etc. and to make sure that you do not run out of money when they retire.

HealthyHealth is an InsurTech operator founded in 2017 by Luca Schnettler. It is based in London and has a staff of 15. Right from the start the operator's objective has been to innovate the insurance sector through digital tools, make policyholders healthier and prevent behaviour which is hazardous to health. HealthyHealth uses digital data, social media data, medical data, emotional data etc. from gamification, music preferences, apps and register data etc. to identify risks and risk profiles and to prevent risks by preparing individualized disease-preventing programmes/health programmes to prevent long-term illness from occurring.

Founder and CEO of HealthyHealth, Luca Schnettler, at Insurance & Pension Denmark's annual meeting on 15 November, 2018.

The business model is based on data collection from a large number of digital data sources – up to 600.000 data per customer per year, such as lifestyle data (in collaboration with business partner GAMIN), social-emotional data via music apps, social media for preparing loneliness scores, gamification data, health data, location data etc.

These data are compared with a pool of data for more than 40.000.000 users, of which 1.000.000 are especially detailed on more than 1.000 variables. Comparison of the unique data of each individual creates the risk profile of the individual including percentages, showing percentages for certain timeframes for diseases, risk of hospitalization and mortality.

In this way, the cost of underwriting is reduced significantly.

> *We should encourage people to share more data because it actually has a lot of benefits. Data can make the world a freer place if people lose their stigma about keeping their data to themselves."*
> – Luca Schnettler, CEO & Founder, HealthyHealth

The advantages to the policyholders – who share their data to obtain these advantages – are that it becomes easier to take out an insurance. You do not need to go to the doctor for blood samples etc. Moreover, the risk profile makes it possible to see which secondary diseases a patient hospitalized with cardiovascular diseases, for example, may develop within a relevant timeframe and, consequently, initiate preventive measures already from the first admission to a hospital, minimising inpatient stay in the long term.

> *In fact, there is a lot of research out there saying that the big killer in the late age stages is loneliness because it impacts your physical health as well as your mental health. So, it was really important for us not to just look at the lifestyle side - measuring heart rate and so on – because you don't get a clear enough picture of the individual's health."*
> – Luca Schnettler, CEO & Founder, HealthyHealth

Based on data and algorithms, HealthyHealth offers individualized health plans aimed at preventing risks from materializing.

> *The thing is that everyone has different risks and each risk that you have should be prevented in a different way. If you apply the same prevention methods to different medical conditions, they will not be as effective."*
> – Luca Schnettler, CEO & Founder, HealthyHealth

The case, therefore, illustrates how new data constantly challenge and expand the potential scope and value offers of the insurance and pensions industry. We do not know what will be possible in just five years, so there may be good reason for allowing insurers to expand their value chains to make the business match the new opportunities for health offers and preventive counselling that appear in the new world.

> *You can connect your music apps to the system, you might connect your social media accounts to it, you might have little gamification tests in there where you slide cards about how you feel and stuff like that. And it's always a work-in-progress because in five years there might be a wearable which can measure how depressed you are during the day or what do I know. It basically about being able to identify new trends."*
> – Luca Schnettler, CEO & Founder, HealthyHealth

What is the industry's responsibility with regard to health data?

The case also raises the question of data-sharing in a health system characterized by complex interaction of actors and by sensitive data being shared by the individual in his or her best interest and – in an aggregated pool format – everyone else's. With that, the case first and foremost emphasises the importance of data security if the infrastructure in such a system is to function.

Secondly, the case offers perspectives of what we today call health data, which are dealt with very cautiously by Danish insurers and other actors. This type of data is sensitive and personal. Another more collectively-oriented way of referring to these data is as 'welfare data': Data that to the individual and in aggregated form offer considerable advantages to everyone in society within key welfare areas such as health, safety, social safety net and a good life after the labour market, financially as well as in health terms. So, extending the value chain with health data and

preventive services is also closely linked with major ethical and legal questions about a common data pool that may benefit us all.

> *In 10 years no one will care about their data being shared with others due to two things: First of all it will be much more secure and you will be in more control of what you want to share or not; and second of all, people will realize that sharing your data actually has more benefits than keeping it to yourself."*
> – Luca Schnettler, CEO & Founder, HealthyHealth

With the enormous growth potential of IoT, data sharing will be of key importance to the future of the insurance and pensions industry. Nor is it unlikely that customers' control of their personal data will increase, which is an important ethical precondition for data-based regulation of behaviour taking place in a responsible way. More and more operators offer security infrastructure to the users – such as encryption technology etc. – e.g. Privacy Enhancing Technology (PET) and Personal Data Stores (PDS). More and more large operators will begin to compete on parameters about giving customers the incentive to share data with them, and GDPR cannot be changed. Within that scenario it becomes paramount for the operators within the industry to identify and strengthen the parameters to ensure that customers will share data with them12. . Such data sharing, however, also entails an ethical dilemma with respect to the regulation of behaviour. As illustrated by this case, data sharing may be beneficial to the individual and desirable for the collective/society but may also be seen as significantly interfering with the individual's self-determination and freedom.

> *When you monitor people, it clearly affects their behaviour, but a great part of this change of behaviour, emerging because you feel controlled, is not always reasonable or professionally sensible as it is often based on very slim foundations."*
> - Thomas Ploug, professor at Aalborg University and former member of the Danish Council on Ethics

The case also illustrates how extending the value chain to include more preventive counselling is a key element of insuring property and life. And it is especially within these areas that major gains from data sharing – especially sensitive data such as health data – become evident.

Data security and extension of the value chain towards more preventive counselling seen from the three positions

The need for the many new data points is indefensible in position 1. Here many will see risks of putting behavioural data into the hands of the insurer. This cannot be defended.

Change of behaviour based on informed and consent-based data-sharing is legitimate in position 2. The case also shows how such regulation of behaviour may become more defensible when tailored to the individual's situation and, relevant, personal matters through maximising data for the purpose of personalizing counselling. More data may, so to say, lessen negative consequences of data-based behaviour regulation, because the change of behaviour becomes more well-founded and beneficial.

In position 3, using especially health data may be defended in utilitarian terms by virtue of the many benefits to society and the health sector of aggregated health data to prevent and treat diseases. The case, thus, also illustrates how the insurance industry may use 'welfare data' from the perspective of both in terms of both ethics of duty and utilitarianism at the same time. In position 3 behaviour regulation should be used to the maximum for the benefit of the community above all.

Summary: Greatest opportunities and challenges of prevention

- The HealtyHealth case first of all illustrates how data-sharing and monitoring highlights 'behaviour regulation' as a fundamental theme of data ethics involving opportunities as well as challenges.

- The case illustrates the many ethically justifiable gains from insurers and pension operators offering preventive counselling. Many Danish operators are already doing so today to a very large extent.

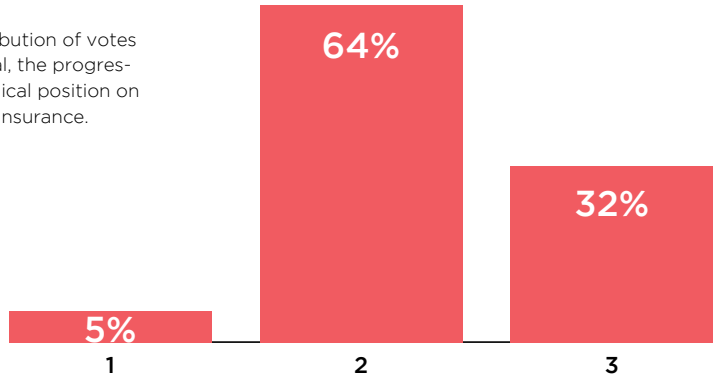
- The individual may – through use of data – change his or her behaviour and obtain lower premiums, better prospects of life and become less of a burden on the community. The latter represents an enormous ethical challenge in terms of value creation and utility benefits to individual and society. Here the individual's ' control of personal data" plays in as a funda-

mental theme of data ethics and a precondition for data-based behaviour regulation – in order that the individual, on a transparent basis, may choose to share or not share – being justifiable in terms of ethics of duty.

- Behaviour regulation, however, may also be unfair, senseless and even wasted because of the customer's lack of knowledge of what works and what does not work (diet, exercise, driving etc.)
- However, the case also illustrates the possibility that, using more and more data, we may be able to prepare better and more sensible, individualized action plans, enabling the policyholder to change behaviour on a more accurate basis.
- The case, moreover, illustrates that 'data security is a fundamental ethical theme which will become a decisive factor for additional data sharing and, together with IoT and more data sources, for access to data and better tailored insurance products as well as behaviour-regulating products.
- In this scenario, insurers will have to focus on the factors (transparency, advantages, security etc.) that affect data-sharing and not least that data are true.
- For customers to accept sharing data with operators to the extent illustrated by the case, extending the value chain, especially into the health sector, will be an opportunity for the industry.

#data ethics

Figure 12 shows the distribution of votes on respectively the critical, the progressive and the offensive ethical position on prevention in the field of insurance.



Prevention debated at Insurance & Pension Denmark's annual meeting, 2018

At the annual meeting of Insurance & Pension on November 15, prevention was debated. Figure 12 illustrates that the majority believed that the progressive position, allowing the greatest possible level of data sharing with the individual in control of his or her personal data, was the right approach. However, 32% believed that the industry should go even further and, based on special authority to use data, get access to e.g. public register data for the purpose of better prevention, counselling and claims administration.

#data ethics

The picture shows CEO of PFA Pension, Allan Polack, on the main stage, commenting the debate on prevention

"With prevention we may also get far taking the position shown above [position 3] by sharing some data, enabling the individual to use the data for the common good. But anonymized when dealing with the data collectively."
– Allan Polack, CEO PFA Pension

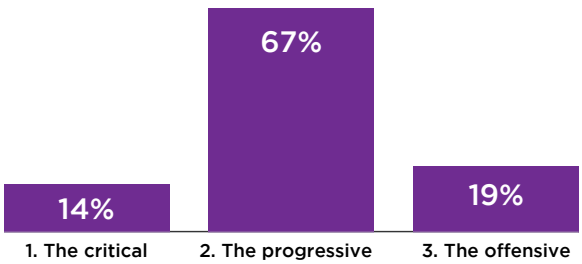
In most cases, real prevention of disease and life events requires personally identifiable data points. But it is possible to achieve major collective advantages by sharing your data anonymously, thereby enabling insurers and pension operators to identify trends and patterns which, ultimately, may result in better products for the benefit of the collective.

#data ethics

Summary of consequences of a natural and predominantly progressive ethical position

A picture is emerging that in several respects the progressive position appears the most natural for an industry that partly carries on business activities based on welfare data and knowledge about risks, partly is an active operator in the Danish welfare society. As far as combating fraud is concerned, the position pulls more in the direction of position 3, because utilitarian values weigh more heavily than concerns based on an ethics of duty.

Especially the need to meet competition from abroad, where data are often extensively used, places demands on the operators' abilities for competitive pricing, effectiveness, provision of sufficient counselling and creation of customer engagement. Of special concern is defining what really constitutes sensitive data.



Discussion of ethical positions at the annual meeting of Insurance & Pension Denmark, 2018

At the annual meeting of Insurance & Pension Denmark on 15 November, 2018, the participants – all operators in and around the industry – were asked to decide which ethical position they thought would best serve the interests of the industry.

Position 1: The critical: 14% believed that this position would be the best basis for a common data ethics.

Position 2: The progressive: 67% believed that this position would be the best basis for a common data ethics

Position 3: The offensive: 19% believed that this position would be the best basis for a common data ethics.

Figure 13 shows the result of the vote on which ethical position the industry should use as a basis for preparing a common data ethics. The total number of votes was 125.

#data ethics

The picture shows Minister of Public Sector Innovation and member of the Danish parliament, Sophie Løhde, COO Tryg, Lars Bonde, Director of the Danish Consumers' Council Tænk, Anette Christoffersen, and CEO of PensionDanmark, Torben Möger Petersen debating consumer protection, privacy and welfare.

"Speaking of data ethics, we need to have transparency, which is not the same as 'Google transparent'. I rather like this blackboard shown in the film with Progressive Patrick [reference to Insurance & Pension Denmark's infographic 13, "Towards a common data ethics", on which 'progressive Patrick' illustrates the progressive position 2], where you can clearly see what you've agreed to. We say that it must be transparent. We must always have more products, so that the policyholders can pick and choose, and, of course, we have to protect their data very well. I actually believe that this way there is no risk that we end up with groups of uninsurables. We say to people: "You can get up to 30% discount if you drive decently. Is this what you want? If not, we have another product." And this summer we asked 4.000 of our policyholders what they thought about it, and 51% actually say that they are interested. So, we can see that this is what our policyholders want."
– Lars Bonde, Group CEO, Tryg

Picture from the film: "Towards a common data ethics of the insurance and pensions industry", illustrating the ideal of the policyholder's control of personal data (in accordance with position 2)[14].

Sensitive data from underwriting to claims payment

Estonia has come a long way with respect to digital citizenship, and the digital world is well-integrated with citizens, companies and society. In Iceland, the health authorities are working on a project that, from 2020, will allow citizens access to downloading their own health data via a common platform. This will make data on allergies, medication and diagnoses etc. accessible and will be linkable to self-reported data on blood sugar, blood pressure

etc. The intention is to make the individual handle his or her health15. In Germany, establishing a common health database is being considered, and, as mentioned, a UK database against health fraud is already in process. 16 However, these and many other similar initiatives do raise the question of which types of data are used and how.

Sensitivity with respect to data types is a particularly important area with considerable ethical implications when used in insurance or pension cases. Figure 14 shows a total overview of data types and their respective degrees of generally perceived sensitivity among European and American customers.

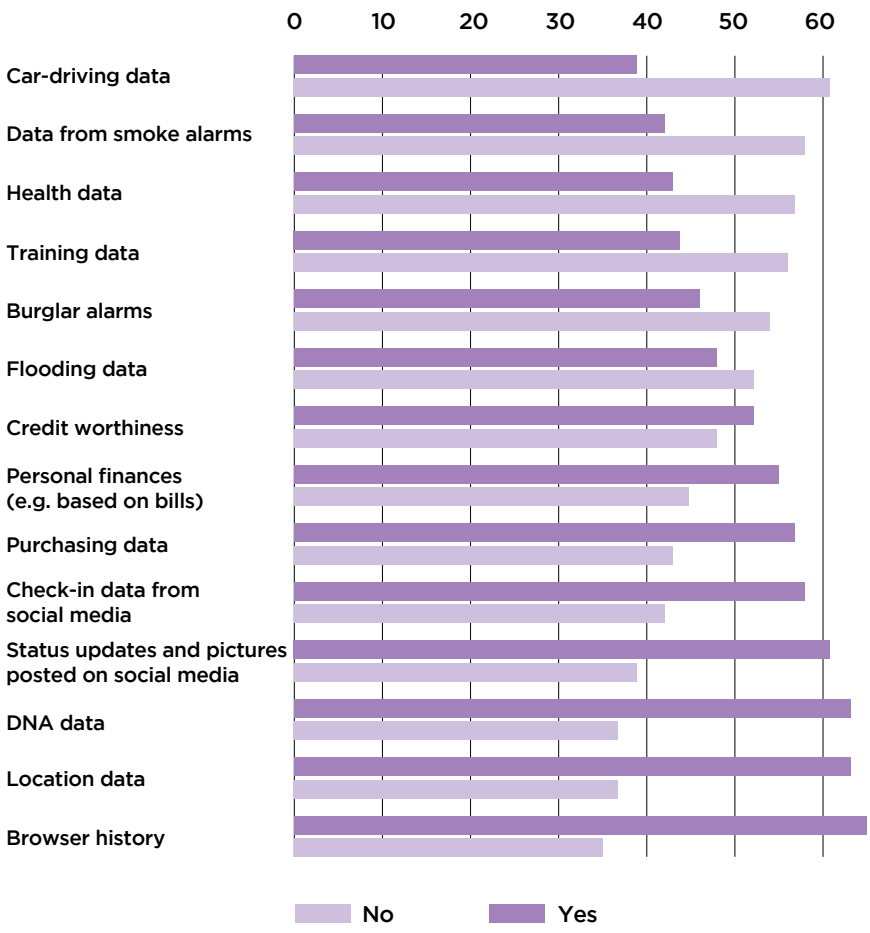


Figure 14 is the result of a survey carried out by Celect in which European and American consumers were asked how willing they would be to share different types of data.

As appears, there are more people willing to share parts of their health data than there are people who do not. Looking at DNA data, there is a clear majority who do not wish to share these data. Above all, figure 14 illustrates the lack of consensus on what constitutes sensitive data. Secondly, the figure shows that the types of data that most people are willing to share are typically associated with value transactions, such as training data, driving data, data from smoke or burglar alarms. At the opposite end are the data types that people are less willing to share, such as location data, browser history or DNA data. These data are not in the same way linked to something that can offer the customer direct value. The survey, however, does not take people's attitudes to correlation of different data into account.

"When you have financial data, location data, activity data, health data, medical data etc., you have an accumulation of data which in itself becomes enormously sensitive."
– Anette Høyrup, senior legal adviser and privacy expert, The Danish Consumers' Council 'Tænk'; vice president of the Danish Council for Digital Security

In Denmark, we have chosen to be especially protective of public-register health data. And there may be many good reasons for that, but also clear ethical challenges posed by the way we do things today when insurers or pension operators need access to health data. In such cases, we are forced to use very insecure procedures of handing and sharing the health data that insurers are legally entitled to obtain in connection with indemnity cases, for instance. As mentioned – from the point of view of the industry – this constitutes an important ethical problem of data use that we need to solve through better private-public interaction and digitalization.

The volume of health data is expected to triple in 2020, and the enormous growth of connected devices worth more than DKK 50 bn, consisting of 1 trillion sensors in 2020, will increase the quantity of data significantly; and several observers are saying that health sensors will constitute a large part of this growth. In Denmark at the present time, IoT is mainly used for buildings, e.g. water pipes. This is mainly because the property area is less sensitive.

"You can look upon health data as either a risk, and hence something requiring a high level of protection, or you can look at it as an asset with a value we ought to exploit. And if we dwell too much on the former definition, we shall miss the train of opportunities and value-creation. And by far the majority of legal work and legislation is reactive, reacting to what has already happened, so if we do not at the same time consider data as an asset, and use them in that way, we fail to learn how to organize legislation and interpretation of GDPR."
- Claus Rehfeld, entrepreneur and Ph.D.

What we consider as sensitive data is history and culture bound, and history shows that perceptions change over time. In this context it is possible to see a significant ethical distinction between, on the one hand, data use relying on data points for prevention and behaviour regulation, and on the other hand use of data where data points that cannot be affected may have a significantly negative effect on individual premiums. Such data points – e.g. on hereditary diseases – are already used in the context of underwriting, but it will also become possible to go further along those lines, which are justifiable in utilitarian terms but not with respect to ethics of duty. Therefore, we probably need to draw a line here. But when we move into the field of claims payments, where an incident may result in a major loss of earning capacity and quality of life, there is a special ethical obligation to grant the industry quick and easy digital access to specific and well-defined sensitive data for the purpose of concluding the indemnity case as quickly as possible and safeguard the citizens' well-earned financial safety net and help them get back to work as quickly as possible rather than end up in isolation due to long-term illness and medical treatment. In other words, there is a fundamental dilemma between, on the one hand, ethically legitimate protection of health data in connection with underwriting and risk assessment, and, on the other, the same protection complicating an ethical obligation to ensure that people in a very difficult situation get the compensation and financial safety net to which they are entitled. So, there is a major ethical problem in connection with private-public collaboration and digital infrastructure, most recently illustrated in the proposal for an amendment of the Danish health act[18]."

#data ethics

The picture shows Minister of Public Innovation and member of the Danish Parliament Sophie Løhde and COO at Tryg Insurance Lars Bonde debating consumer protection, privacy and welfare.

Debate on protection of the privacy and welfare of citizens at the annual meeting of Insurance & Pension Denmark, 2018

At the annual meeting of Insurance & Pension Denmark on 15 November, 2018, the theme of how best to protect the privacy of citizens within the perspective of a data ethics was discussed.

"If you ask me whether the insurance operators must have access to the citizens' health records at sundhed.dk, the short answer to that question is a clear no."
– Sophie Løhde, Minister for Public Sector Innovation and member of the Danish Parliament.

Especially the theme of allowing pension providers access to health data was debated; and improved private-public collaboration was encouraged.

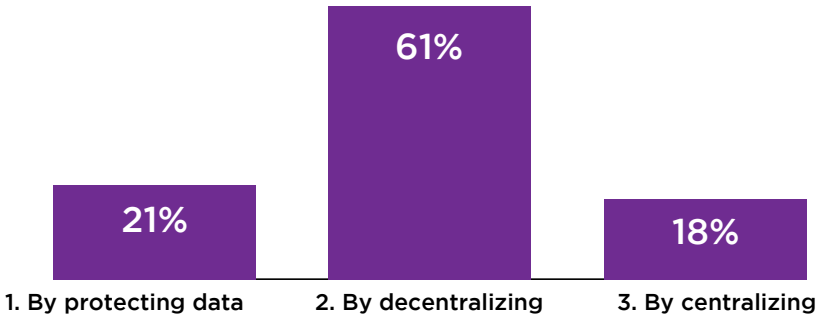
"The authorities responsible for sundhed.dk (a national health site) have organized matters in such a way that, as a citizen, you can only give consent to sharing your health data with other health authorities such as doctors or hospitals. You cannot give it directly to us. So, if we are to have access, we must write to the hospital where the policyholder has most recently been admitted, and subsequently the hospital – in the old-fashioned way – will send us the documents required. I think that you [Sophie Løhde] should tell the Danish regions, who own sundhed.dk that the data belong to the citizen, and if the citizen wishes to share his or her data with us, the citizen should, naturally, be entitled to do so."
– Torben Möger Petersen, CEO of PensionDanmark

Also, the criterion on specificity, delimitation and relevance of data access was debated:

"I do not want you to have general access, but I'm prepared to look at the possibilities for, in the long run, designing a wiser solution to how we take out the smaller quantity of relevant data and share them in a wiser and smarter way."
– Sophie Løhde, Minister for Public Sector Innovation and member of the Danish Parliament

Subsequently the audience voted on which fundamental approach to the citizen's data would be best suited to safeguarding both privacy and welfare: By means of respectively protecting data, decentralizing, to make the citizen responsible for his or her personal data, or centralizing on public hands with a view to getting an overview and access.

Figure 15 shows the result of the voting.
117 voted



The result of the vote, in which one in five voted for the first option of protecting the citizen's data, indicates that sensitivity with respect to health data, with which the debate was concerned, is of importance in terms of taking an ethical stand. It is interesting that 61% voted for an especially progressive ethical approach to storing and sharing of sensitive data. An approach that, in contrast to the other two options, is furthest from the infrastructure we know today.

It is the customer's data: Privacy by Design

"If you have a 100% private and fully secure library of all of your data. The perfect data. Why would the companies go around your back for data elsewhere, which is thin, unreliable, not permissioned and expensive when they can go directly to you and ask you for your data. Explaining how they will use it and not use it and what they want to give you back in terms of value exchange. Then the individual is in control and this changes everything."
– Julian Ranger, Chairman & Founder, Digi.me

It is in the policyholder's interest to control personal data and what should be shared with the insurer. It is more ethically right that the policyholder owns, has access to and control of personal data. In contrast to other operators, such as auto companies collecting and getting access to driving behaviour without asking the customers. Or tech giants like Facebook and Amazon monopolizing data produced by users on their platforms, giving them competitive advantages over the insurance and pensions industry.

"We need better access to the data held by public authorities. Establishing personal ownership, also of publicly held data, will be of great assistance to the industry."
– Per Jensen, head data and analysis, Tryg

The most commercially interesting data are the personally traceable data. This does not imply that aggregated and anonymised data, such as statistics, cannot or should not be used to analyse demographics etc., but the concrete house data, car data or data about individuals are of the greatest interest, and the individual should have greater opportunities for sharing more of these data with the insurers if he/she wishes to do so.

"The core thing I would advocate for if I was in insurance would be – building on the GDPR and the right to have your data erased – the right to ownership. And the reason for that is that it would help for more data proliferation. Which is ultimately what we want in the insurance industry – we want to know everything about everything. While the right to erase gives people agency over data that they publish, it does not give people the right to things that derive from them. And it can reduce the amount of data that exists out there, which affects the understanding that we need to identify risk and transfer risk."
– James Felton Keith, Author & President, The Data Union

We recommend that the industry fully adopt the principles of Privacy by Design (PbD). This does not mean broad access to all health data but only to the specific, relevant data needed in connection with the administration of a specific claim.

"Those who are able to put the total value package together and link it to a reasonably noble purpose with an excellent customer experience, compliance, high ethical standards – both as business model and in terms of data processing – will win. An millennials will intuitively be capable of decoding those things in next to no time."
- Sam Kondo Steffensen, program manager, DTU Business

In the long term the policyholder will, hopefully, easily and transparently be able to allow the pension operator access to SKAT (the Danish tax authority) to provide information about income and housing, and Pensionsinfo, which holds information on matters relating to pensions. Ideally, married state (SKAT and Pensionsinfo) would also be included via NemID (common secure login) and consent. Account information would also be potentially relevant data for ensuring optimal financial security for the citizen if he or she wants counselling of that order.

"I believe we are going to see a gigantic market for what is called privacy enabled products, which include consumer control of data owned by the consumer, enabling him or her to do with them what they want, which might include sharing them with an insurer, sell them etc."
– Anette Høyrup, senior legal adviser and privacy expert, the Danish Consumers' Council Tænk; vice-president of the Danish Council for Digital Security.

"As an industry we have no interest in crossing the boundaries of policyholders and becoming 'creepy'. We do things completely openly and transparently – 'you get this or that type of service if you provide these or those data'. And if the policyholder has second thoughts, you just swipe back again.
– Morten Lund Madsen, CFO, Sampension

PbD represents a different way of working with GDPR and data compliance. But this is about more than law and compliance. It is about a multi-disciplinary approach combining several parameters in one value universe.

"We have to be creative in exploring the possibilities of the General Data Protection Regulation. Protection of personal data, of privacy, is not the work of the technician, it's not the work of legal, it's not the work of economics or politicians or business, but all of them together. You need a multidisciplinary approach and work together to really make it, because it is technical, it is economical, it is legal. You have to have a good mix of these people and working together to achieve a very good system[19]".
– Willem Debeuckelaere, President, Belgian Data Protection Authority Vice Chairman, European Data Protection Board

In this connection it will be relevant to have more and better technological platforms to ensure individual rights and access to personal data.

We are referring to Personal Data Stores (PDS). Data platforms gather, clean up and organize datasets and data streams safely and in a central place20 One example is Data for Good Foundation. This is a Danish example of a commercial, non-profit foundation in which health data, behavioural data, illness and accident data paired with SoMe data are made available to individuals. In this way insurers and pension operators may get access to anonymised datasets but also to personally relatable data with a view to offering better personalised counselling services[21].

"If we look 10-15 years ahead, we need to ask ourselves who owns the customer relation. If all data are shareable, there is a risk that the operators end up as infrastructure while a number of data brokers, trusted by the policyholders, own the customer relation. It is a matter of time before we will be facing that challenge, I believe. The fight we are presently fighting over the customers will then be completely different."
– Morten Lund Madsen, CFO, Sampension

Developments are already happening within this field, and PDS is one of the Siri Commission's recommendations[22]. That more control of personal data may lead to more participation and data sharing – which in turn may create value for the individual, the collective and the companies – is one thing. On the other hand, it may also lead to less data sharing. That is the most utilitarian concern about PDS. However, the heaviest ethical argument for a PDS is the argument from ethics of duty, according to which the individual, as an objective in itself, acquires ownership of the data that can be traced back to him or her. However, control of personal data – with or without PDS - presupposes a certain amount of digital education, making this an important task, too, for the industry in the future digital economy.

Insurers play a huge role in terms of driving the market in the right direction – both with respect to privacy and to ensure optimum use of the many unexploited data points. If they wish to do so, they may take the lead with this privacy agenda."
– Anette Høyrup, senior legal adviser and privacy expert, the Danish Consumers' Council 'Tænk'

The industry's ethical principles for use of data

Throughout the analytical work carried out towards a common data ethics, it has become clearer that, ethically, the industry should:

- Identify and more accurately calculate far more risks for the policyholder's own good, because those risks 1) may be affected and minimised, 2) because they are covered in solidarity in return for a premium, and 3) because they create more fairness in the pools.

- Combat fraud with the necessary means and with the greatest possible use of technology to reduce the number of false-positives.

- Use data to predict and prevent claims within the fields of property and personal injury if the policyholder so wishes.

- Support both the individual and the welfare society with prevention and knowledge, including interaction between the public sector and the operators.

- Ensure that use of data takes place with the greatest possible transparency, security, specificity and delimitation as well as giving the individual the possibility for staying in control.

- The industry has an ethical obligation to obtain the specific and necessary data in order to handle claims and indemnity payments, especially when it comes to personal injury where data are often sensitive and therefore well protected in public registers. For this reason, we consider it to be good ethics for the industry to strive to ensure effective digital, secure, specific as well as consent-based sharing of especially the very sensitive but essential personal data.

Placed within the model of data ethics, this provides the following illustration of where the industry is in ethical terms.

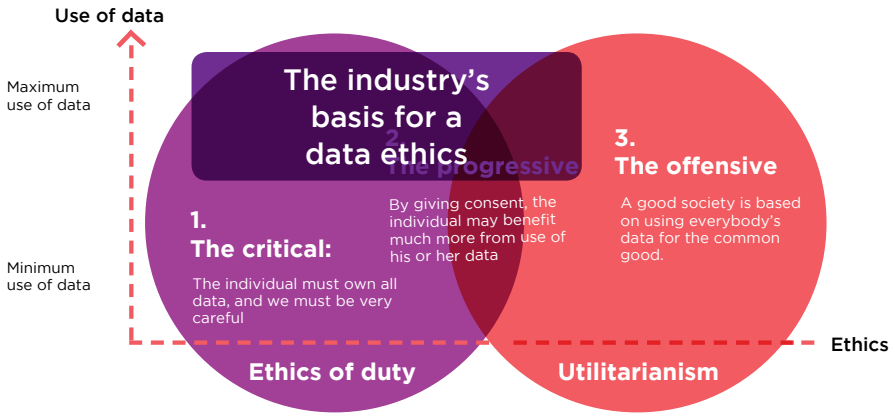


Figure 16 shows the industry's basis for a data ethics. The main emphasis is on arguments from ethics of duty, but the mixture of arguments from utilitarianism and ethics of duty means that more data can be used first of all to achieve ethical objectives relating to duty but also utilitarian objectives. Customer expectations, data regulation and international competition exert further pressure in favour of a position based on maximum use of data based on ethics of duty – keeping the individual at the centre.

The industry's ethical compass

Trust between citizens, the authorities and the industry is fundamental if the insurers are to be able to insure property and life and support the welfare society. Therefore, the industry has no utilitarian interest in using data in ways challenging that trust. And from the point of view of ethics of duty, it ought to be a clearly defined task for the industry to create high digital security, refrain from reselling policyholders' data and only use relevant, specific and concrete data needed for claims administration. In this context, digitalization plays a key role in ensuring different types of access, through role management etc., and consequently a progressive data ethics would also need to make considerable allowances for the opportunities provided by technology and digitalization.

Among the many possible ethical principles laid down in the different recommendations, our analytical work and, especially, the three case studies have produced five themes of special relevance to the industry – both seen in isolation and in interaction with each other – and which all in a way constitute prerequisites for trust. How to relate to these fundamental themes depends on the ethical position from which you speak. The five themes, and the questions they prompt are:

1. Digital security – can I be sure that my data will not end up in the wrong hands?

2. In control of your personal data – am I in control of my personal data, and who has access to my private life, and for what purposes are the data used?

3. Personalization – will I be exposed to segmentation/profiling in a way that will be beneficial for me or not?

4. Behaviour regulation & incentives – will I change behaviour for better or worse (depending on how sensible the change of behaviour is) as a result of sharing data and being monitored? And are there financial incentives for me – or some sort of value transaction – inducing me to share more data, withhold them or manipulate my data to the advantage or disadvantage of myself and/or others?

5. Transparency – do I know where my data are, what they are used for and how? Do I know what I consent to or not when data about me are collected? And do I have a fair idea of the consequences of consenting to data sharing in each individual case?

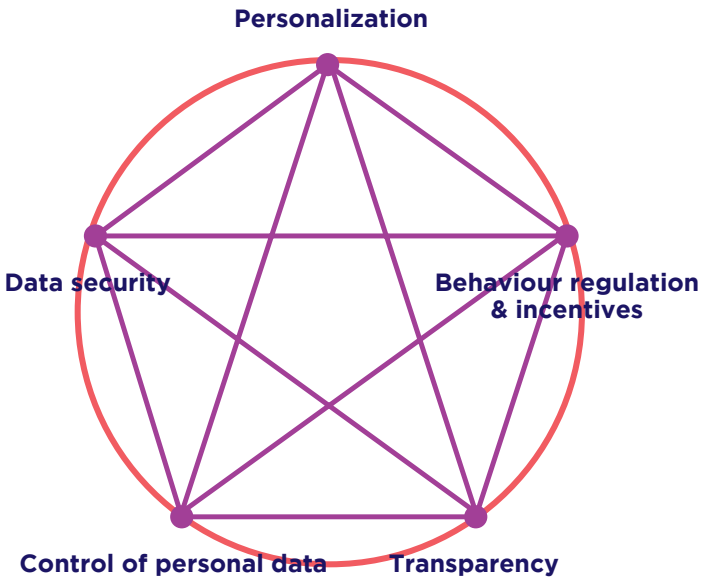


Figure 17 shows the ethical compass. The figure illustrates the industry's five fundamental themes related to data ethics.

The individual fundamental themes cut across the three positions but are, in principle, interpreted and handled differently, depending on the position from which we are viewing them:

1. Data security

Position 1
(ethics of duty+minimum use of data) In principle data security is here mostly viewed as an objective in itself, and minimising use of data is a tool for achieving greater data security. So-called "security through obscurity". Anonymizing may also be used to achieve data security but at the risk of pseudonymization, which means that anonymized data may easily become personally relatable again. Therefore, anonymising is often considered a "dangerous solution".

Position 2
(ethics of duty+maximum use of data) Here, on the other hand, data security is basically seen as an infrastructural precondition for more and better use of data. Since data security presupposes transparency, techniques such as data lineage, i.e. tracking data through systems back to the original source, become important tools. Partly to obtain certainty about security and that data have not been illegally or wrongly used, partly to ensure that the value generated from the individual's data may also be traced back to him or her as the original owner of the specific data.

Position 3
(utilitarianism+maximum use of data) Here data security is likewise seen as an infrastructural precondition for more use of data for the common good, for operators and society. But data security is given greater priority, especially because, for the data manager, great risks are associated with storing large quantities of personal data. In register research, the use of integration of registers may also carry more weight than keeping up security in the systems to protect the citizens.

Recommendation
Data security is fundamental to data ethics. A secure data infrastructure is a prerequisite for sharing data between individual, operators and the public sector. Consequently, Privacy by Design is an important task for the industry in order to

continue digitalisation and for data quantities to continue to grow while keeping the individual at the centre of things. Privacy by Design principles should also be introduced in the public sector, especially with respect to sharing of sensitive data in particularly urgent situations involving indemnity payments. Thus, the industry's approach to data security should be based on ethical position 2.

2. Control of personal data

Position 1
(ethics of duty+minimum use of data). Here control of personal data is in principle the crucial factor. It is based on the right to anonymise data and is critical of any potential monitoring. Control of personal data is primarily interpreted to mean that the individual should not at all be invited to share data. Nor, as mentioned, should an operator be entitled to anonymise data for research and innovation purposes, as this is often associated with so-called pseudonymation, which may be personally relatable, e.g. via *Dictionary Attack.*

Position 2
(ethics of duty + maximum use of data). Here the individual should in principle have the greatest possible control of his or her personal data, and preferably by putting them into play as much as possible in the individual's self-interest. Opt-in-based data sharing is an important mechanism to ensure that collection of data is carried out with the individual's consent and knowledge of consequences. Moreover, the individual should have the possibility of personally anonymising and sharing data for research or innovation purposes, should he or she so desire.

Position 3
(utilitarianism+maximum use of data). Here personal control of data is in principle less important and should not always take precedence over direct access – based on special authority to process information – to registers of person-related data. Opt-out-based data access, however, is a form of control of personal data you would warmly advocate in position 3. Moreover, as an operator or public authority, it will also be possible to use anonymising of datasets for research and innovation purposes in the interests of the collective.

Recommendation
The customer must be at the centre of the operators' use of data, and the customers/individuals/citizens own the personal data. The industry should strive to ensure that data neither belongs to the operators or the public authorities. "Control of personal data" should be a key principle for the industry, because it will be an important tool for preserving trust, which is a key factor for good data sharing between individuals, operators and the public authorities. The industry should strive to ensure that the customer's data are as easily accessible as possible and that that the customer is always in possession of the best possible basis for decisions in order to obtain the right coverage or investment profile and, hence, security. This especially goes for public-register data. More data for more accurate risk assessment is ethically justifiable from principles of both fairness and solidarity. But having personal control of your data is a prerequisite. This means that the industry's position on control of personal data is based on position 2.

Digital education of customers is an important concomitant principle, because attention to new digital risks and advantages (and disadvantages) of data sharing – perhaps to obtain better coverage or avoid cheating yourself or the operator – benefits both the individual customer and the operator. A data-sharing economy based on pseudo-consent is hardly in anyone's interest. And one of the great challenges of position 2 is that it presupposes an individual capable of assuming ownership and control of personal data. A small segment of the population are not, and this is a challenge. Here, digital education plays an important role.

3. Personalisation

Position 1
(ethics of duty+ minimum use of data). Here, data-driven personalisation is, in principle, seen as a risk for the individual. Here, an operator would resist using data to avoid treating an individual against his or her own interests. If personalisation is used in connection with inquiries and counselling with respect to specific life events, it will to some degree be seen as 'creepy' and as being under surveillance.

Position 2
(Ethics of duty+maximum use of data). Here personalisation in connection with underwriting and pricing is in principle seen as an opportunity of giving the individual a more accurate price. Personalization also offers the individual opportunities for obtaining a far better overview and greater security around his or her coverage.

Position 3
(utilitarianism+maximum use of data). In principle, more accurate personalisation is here seen as an important means of aiming the resources of institutions in the right direction in order to create the best possible solutions for the common good.

Recommendation
It remains legitimate to use data to differentiate between the risk profiles of customer segments and identify high-risk groups with respect to both property, behaviour and health. A risk-based price is necessary for two reasons:

- To establish an equal playing field vis-a-vis competitors
- Risk and premium should go together, because this will create the best incentive structures

Use of more data points may be used to break specific and common stigmata/segmentations that may harm the individual in the form of, say, an unjustly high premium. Young car drivers, for instance, may and should have the possibility of influencing a strongly age-specific stigma by demonstrating sensible driving behaviour. The same goes for people with health problems who handle them through monitoring or other treatment.

The limits to tariffing (with respect to personalisation), however, should be established where personal data points, over which the individual has no influence, are used for further (micro)-tariffing and to demand a considerably higher premium of the policyholder. In this case, part self-regulation, part free choice and real alternatives should be key principles for the industry. It already is and should continue to be an important principle for the industry to provide realistic and affordable solutions to those who choose to share fewer data. It is not in the industry's interest that people become uninsurable. A "share data or suffer the consequences" scenario should not be allowed to emerge, and therefore alternatives to products based on sharing of many data should not be discriminatory or put the interests of the individual at stake. A positive vision presupposes that the industry makes an effort to enable everyone to feel at ease in a world of many data and many possibilities for sharing of data.
In the long term, trends within data use may be expected to require that society, through collaboration between operators and public authorities, find durable and just welfare solutions for extreme high-risk groups. However, it neither can nor should be the responsibility of the industry to seek to equalize all existing social as well as financial inequalities.

The ethical approach to personalisation , thus, is based on position 2 – both when maximum use of data is justifiable from the point of view of ethics of duty and when it is not, and we need to draw a line. In the long term, within the context of risk assessment, some areas - especially regarding sensitive data such as location, plot and geodata relating to houses - will slide in the direction of position 3, because the utility value of that knowledge and the potential, beneficial solutions to the individual, society and the insurer will be considerable without compromising the individual.

4. Behaviour regulation and incentives

Position 1
(ethics of duty+minimum use of data). Here behaviour regulation is considered potentially dangerous, because it may harm the individual. And you will be critical of incentives to share data as this may affect people's judgment in a way that may be inappropriate for the individual.

Position 2
(ethics of duty+maximum use of data). Here incentives are key to the individual, affecting his or her life situation for the benefit of themselves in terms of both lower risks and premiums. In this position you regard use of data as more of a means to make specific behaviour regulation even more targeted, relevant and sensible via even more personalized counselling. You will also see incentives to share data as an important part of getting data into play for the benefit of the individual.

Position 3
(utilitarianism+maximum use of data). Here, behaviour regulation is of benefit to society. You will also see incentives to share data as an important theme with respect to insurance fraud, because prevention efforts prompting people to give true information about their claims will have a beneficial impact.

"You can do a genome test, use wearables and sensor data to collect a very large data set on the individual, but you must ask yourself: In which ways is it OK to collect those data? Should we use financial incentives, as we have seen in the USA where you can get 50$ to share data, or do you offer cheaper insurance? But financial incentives tend to affect people's judgment."
– Thomas Ploug, professor at Aarhus University, Ph.D., and former member of the Danish Council for Ethics

Recommendation
Prevention efforts and regulation of behaviour are legitimate, so long as the customer has a free, informed choice and a real alternative to data sharing. In addition, the industry should have possibilities for using large quantities of data to support welfare society save on medical expenditure etc.

It is ethically justifiable with respect to both the community/solidarity and the individual for the industry to store and use the data required to combat fraud. Artificial intelligence may contribute to reducing the number of unjustly monitored individuals, and, consequently, the technological development and the development of automatic aggregation and analysis of data points in connection with claims administration and anti-fraud will be a priority area for the industry and its operators. Sharing of data between operators and public authorities in fraud cases will be an important focus area for the industry, too. Also, encouraging the customer to provide true and 'correct' data is an important principle that applies to underwriting but particularly to claims reports and efforts to prevent fraud.

The industry's approach to using data for regulation of behaviour and incentives, thus, is based on position 2, where the individual has the choice whether to allow data to be used for prevention and regulation of behaviour. But especially when it comes to prevention, in broad terms, the industry may base its approach on position 3, where concern for the collective outweighs concern for the individual. Technology, however, also ensures that the two views do not conflict directly with each other.

5. Transparency

Position 1
(utilitarianism+maximum use of data) In principle, transparency is not so important, as you would, basically, refrain from using more data. Concern for privacy and anonymising are of much greater importance than transparency, which only becomes relevant when data are used.

Position 2
(utilitarianism+maximum use of data) In principle, transparency is a key component of achieving data security, but also of making the individual capable of using personal data on an informed basis. Here, the desire for personally controlled and, thus, transparent data systems (e.g. from the Mydata movement) is crucial.

Position 3
(Utilitarianism+maximum use of data) Here transparency will be important, too, but primarily to achieve a high level of digital security and, thus, minimise risk of storage and administration of large quantities of data. In position 3, transparency will also, as a principle, be seen as a means to preserving and strengthening the relation of trust between data subject and data administrator to ensure that data may continue to be used for the benefit of the great majority.

"There's a rising belief in the right to both data privacy and data security. However, achieving both are illusions. Security is impossible without increased monitoring – and, thus so is true privacy. We should shift the focus towards data empowerment by giving people control over their data and a mechanism to retaliate if it is used in an inequitable way."
- Steven Schwartz, Managing Director, CEO Quest

Recommendation
Transparency of declarations of consent and informing about access to data is a key principle. If the operators want access to people's data, 'pseudo consent' is not the way ahead. Operators have an interest in – as well as an ethical obligation – to make it easy and understandable to what the customer gives his or her consent. This also involves a demand for greater transparency of risk assessment processes, including information about which data points the operator uses to assess risks associated with the individual customer. Trust may to a certain degree replace transparency, while lack of transparency may ultimately erode trust.

For these reasons, the industry ought to look at principles of legal by design and ethics by design, where principles, consequences and purposes of consent appear transparently and in a user-friendly manner. The industry's approach to transparency should be based on position 2. Transparency – combined with data security and control of personal data – is more important than rigid focus on privacy.

Towards a common data ethics

"It is a scary reality when everything can be known, but we are already living in that reality, so we need to have an open and honest conversation about this fact."
– James Felton Keith, Author & President, The Data Union

With this report, we have tried to outline the first steps towards a common data ethics. We have attempted to define the framework and the first important principles of how data and ethics interact in an industry concerned with important tasks related to individuals, society and business interests. We have tried to take up the most difficult discussions at the annual meeting of Insurance & Pension Denmark, and we have discussed, listened and tried to nuance the ethical themes in collaboration with around 275 participants from inside as well as outside the industry, and we have listed and discussed with people from at home and abroad.

We have attempted to point to boundaries that must be set and openings where we can and must do more with data. And in a world where IoT and algorithms have already significantly begun increasing the quantity, applicability, opportunities and risks of data use, we see this as an important forward-looking step to have launched a positive discussion in collaboration with Insurance & Pension Denmark on what the industry does, can, should and will do with data. In the public debate, data ethics is often about what to use less of. But this report has made clear that there are great opportunities of using data that we can and should make greater use of – in the interests of individuals, society and business.

The insurance and pensions industry should contribute to creating welfare solutions in response to our various modern problems, and that often requires more intelligent use of data. Using data must be possible in full respect for the individual and the common good. And without anyone being left in the lurch. Data can and should be used for the common good of the individual and the collective, and it must be done while keeping the rights and options of the individual at the centre of what we do.

Interviewees:

Anette Høyrup,
Senior legal adviser and privacy expert, Danish Consumers' Council 'Tænk'; dept. chairman, Council for Digital Security

Björn Hinrichs,
Executive Director, Informa, HIS & Vice-president, Arvato Financial Solutions

Bo Søvsø Nielsen,
Director, Shift Technology

Brian Egested,
Head of dept. and member of the board of directors, Alm. Brand

Brian Wahl Olsen,
Director of Claims Skadeservice, Alm. Brand

Claus Rehfeld,
entrepreneur and Ph.Ds.

Flemming Tovdal Schmidt,
Director of Customers, Customer service and & IT, PensionDanmark

Harald Bjerke,
Manager at Fraud Prevention Office, Finans Norge

Henrik Bundgaard,
Claims Director, Codan

James Felton Keith,
Author & President, The Data Union

James Neville,
CEO, Citizen

Jon Cooper,
Co-founder & CEO, Life.io

Jon Johnsen,
Group CEO and COO, PFA

Julian Ranger,
Chairman & Founder, Digi me

Lars Bonde,
COO, Tryg

Luca Schnettler,
CEO & Founder, HealthyHealth

Matteo Carbone,
Director of the IoT Insurance Observatory (previously Connected Insurance Observatory), Global InsurTech Thought Leader & Investor

Morten Lund Madsen,
CFO, Sampension

Norman Black,
EMEA Insurance Industry Principal, SAS

Per Jensen,
head of data and reporting, Tryg

Povl Heiberg Gad,
Ph.D. fellow at CBS

Ravi Vatrapu,
Professor & Director, Centre for Business Data Analytics, Copenhagen Business School

Sam Kondo Steffensen,
program manager, DTU Business; IntraWorld Holding Intl.; member of the board of directors, Innovatic Business Software

Steven Schwartz,
Managing Director, CEO Quest

Thomas Enna,
Senior Vice-President Business Development, Topdanmark

Thomas Ploug,
professor at AAU, Ph.D. and former member of the Danish Council for Ethics

Vagn Jelsøe,
dept. director of Politics & Campaigns, Danish Consumers' Council 'Tænk'

Special thanks to the panellists at the annual meeting of Insurance & Pension Denmark, 2018:

Lars Bonde,
COO, Tryg

Torben Möger Petersen,
CEO, PensionDanmark

Anette Christoffersen,
CEO Danish Consumers' Council 'Tænk'

Sophie Løhde,
Minister for Public Sector innovation and member of the Danish Parliament

Allan Polack,
CEO, PFA Pension

Peter Hermann,
CEO, TopDanmark

Vivian Lund,
Group CEO

End notes

1 (Floridi, 2013; Floridi & Taddeo, 2016)

2 https://www.accenture.com/t20161011T222718__w__/us-en/_acnmedia/PDF-34/Accenture-Pulse-Check-Dive-Key-Findings-Personalized-Experiences.pdf

3 Afgift reduceret (charge reduced) 2019, Finansloven 2019 (Danish budget, 2019)

4 Mydex CIC Data Portability whitepaper, June 2018

5 Mydex CIC Data Portability whitepaper, June 2018

6 "Big Data is coming - are you ready? The European Actuary no 15 -Oct 2017, s. 5-7

7 "Big Data is coming - are you ready? The European Actuary no 15 -Oct 2017, s. 5-7

8 Oplyst forsikringssvindel I Danmark (Insurance fraud in Denmark) – report 2018

9 https://www.shift-technology.com/hicfg_selects__shift/

10 https://borsen.dk/nyheder/generelt/artikel/1/359807/deling_af_motions-data_koster_kvinde_hendes_forsikring.html?hl=YTozOntpOjA7czoxMDoiZm9yc2lrcmluZyI7aToxO3M6OToiRW5kb21vbmRvIjt-pOjI7czoxMDoiRm9yc2lrcmluZyI7fQ,,

11 https://www.aig.com/knowledge-and-insights/newways-to-fight-fraud

12 "The Data Sharing Economy: Quantifying Tradeoffs that Power New Business Models", AIG

13 https://www.youtube.com/watch?time_continue=175&v=cKU7ViBGHqE

14 https://www.youtube.com/watch?time_continue=175&v=cKU7ViBGHqE

15 https://dattacalabs.com/decentralizing-healthcare/

16 https://www.shift-technology.com/hicfg_selects_shift/

17 Future Agenda – "Future of Patient Data", insights from multiple expert discussions around the world, 2018

18 https://prodstoragehoeringspo.blob.core.windows.net/e684333f-e340-4e9a-99f9-dc395a02d3aa/Lovforslag%20om%20bedre%20digitalt%20samarbejde pdf

19 https://www.youtube.com/watch?v=pO3kp-ii-60U&t=11s

20 https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/creating-a-successful-internet-of-things-data-marketplace

21 Tranberg P. og Hasselbæk G.: Dataetik – den nye konkurrencefordel (Digital ethics – the new competitive advantage).

22 https://www.version2.dk/artikel/siri-kommissionen-personal-data-store-vejen-frem-trygge-borgerdata-1086186?utm_source=twitter&utm_medium=social&utm_content=wall_post&hootPostID=55e-8395a0366717543fdd47330f11d4c

23 http://nextwork.as/

Referencer

Accenture. (2016). Building digital trust: The role of data in the digital age: https://accntu.re/2OexV9m

AIG. (2017). The Data Sharing Economy: Quantifying Tradeoffs that Power New Business Models: https://bit.ly/2D9T3Ws

Albrechtsen, T. & Bornakke, T. (2018). Vi har pligt til at dele vores data med fællesskabet (We have a duty to share our data with the community Information: https://bit.ly/2y6UPGe

Al-Erhayem, J. (2018). 200 GDPR-mails i min inbox – til hvilken nytte? Børsen. (200 GDPR mails in my in-tray. To what use? Børsen: https://bit.ly/2OVay1x

Andersen, T. (2018). Siri-kommissionen: 'Personal data store' er vejen frem til trygge borgerdata ('Personal data store' is the way to secure citizen data in the future): https://bit.ly/2zwGJzo

Arendt, H. (1994). Eichmann in Jerusalem - A Report on the Banality of Evil. Penguin Books.

Awad, E., Dsouza, S., Kim, R., Schulz, J., Henrich, J., Shariff, A., ... Rahwan, I. (2018). The Moral Machine experiment. Nature, 563(7729), 59. https://doi.org/10.1038/s41586-018-0637-6

Bagger, H (2018) Debat: Tillid til virksomhedernes datahåndtering er hård valuta (Trust in the operators' handling of data is hard currency) Børsen

Bentham, J. (1776). A Fragment on Government. Cambridge University Press. https://doi.org/10.1017/CBO9781139163675

Bundgaard, H (2018) Forsikringssvindlere spilles videre som sorteper (Insurance fraudster: passing the buck) Berlingske: https://bit.ly/2QBrhHD

Burbach, M (2016) Soft Fraud and Possibilities for Prevention. Gen Re.: https://bit.ly/2gBBBSO

Cabinet Office & Behavioural Insights Team. (2012). Applying behavioural insights to reduce fraud, error and debt. GOV UK.: https://bit.ly/2Dkxpk6

Davenport, T H , & Prusak, L (1998) Working Knowledge: How Organizations Manage what They Know. Harvard Business Press.

Deichmann, J , Heineke, K, & Reinbacher, T (2016) Creating a successful Internet of Things data marketplace: https://mck.co/2lAIhjk

Due, B L , Christensen, J H , & Hennelund, M (2018) Du er ikke bedre end dit data Kommunikationsforum (You are only as good as your communication forum). Retrieved from http://www.kommunikationsforum.dk/artikler/Guide-til-databranding

Due, B. L. (2018). Autonome dræbermaskiner og onde datafyrster (Autonomous killer machines and evil data lords) Kommunikationsforum. Retrieved from http://www.kommunikationsforum.dk/ artikler/Moral-som-forretningskritisk-parameter

Durkheim, É (1895) The Rules of Sociological Method (1st American ed.). New York: Free Press.

Floridi, L. (2013). The Ethics of Information. Oxford University Press UK.

Floridi, L , & Taddeo, M (2016) What is data ethics? Philosophical Transactions. Series A, Mathematical, Physical, and Engineering Sciences, 374(2083). https://doi.org/10.1098/rsta.2016.0360

Forsikring & Pension (2018) Opdaget forsikringssvindel i Danmark – rapport (Detected insurance fraud in Denmark – report) 2018

Frank, L (2018) Det elektroniske overjeg (The electronic superego) Weekendavisen

Future Agenda – Open Foresight. (2018). Future of Patient Data - Insights from Multiple Expert Discussions Around the World: https://bit.ly/2JeKizH

Geertz, C. (1977). The Interpretation of Cultures. New York: Basic Books.

Hart-Hansen, K. (2018). Kronik: Forløs dansk sundhedsteknologisk potentiale (Redeem potential of Danish health technology) Børsen

Hart-Hansen, K. (2018). Kronik: Tag livtag med om fordommene om sundhedsdata og bring Danmark i front(Feature article: Wrestle with the prejudices about health data and bring Denmark into the lead) Børsen

Holm-Larsen, T. (2018). Mens Finland tør, står Danmark paralyseret (While Finland dares, Denmark stands paralyzed). Børsen.

Kamallakharan, B. (2018). Decentralizing Healthcare: https://bit.ly/2xlQGOC

Kant, I. (1785). Grundlæggelse af sædernes metafysik (Groundwork of the metaphysics of morals) Copenhagen: Gyldendal.

Kivisaari, E. (2017). Big Data is coming - are you ready? The European Actuary, no. 15 - Oct 2017, s. 5-7: https://bit.ly/2R3Npvg

Kjær, J. S. (2018). LA-spidser efter alvorlige refleksioner: Den dataglubske stat skal have mundkurv på (Liberal Alliance leadership after serious reflections: The data-greedy state must be gagged) Politiken

Lyhne, A. (2018). Børsen mener: #techlash kan også ramme danske politikere (#techlash could also hit Danish politicians) Børsen

Mittelstadt, B D , & Floridi, L (2016) The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. Law, Governance and Technology Series, The Ethics of Biomedical Big Data,445-480. doi: 10.1007/s11948-015-9652-2

MyData Global. (2018, 6, september). Legal landscape and GDPR [YouTube]: https://bit.ly/2xIlfxW

Mydex Data Services CIC. (2018). Data Portability whitepaper.

Nyvold, M. (2018). GDPR udfordrer internetgiganternes datamonopol(GDPR a challenge to the digital monopoly of internet giants): https://bit.ly/2QcEGFR

Philip, A. (2018). Kronik: Vi har ret til privatliv i den digitale verden (Feature article: We have a right to privacy in the digital world) Børsen

Quinn, S. (2008). The Transformation of Morals in Markets: Death, Benefits, and the Exchange of Life Insurance Policies. American Journal of Sociology, 114(3), 738-780. doi: 10.1086/592861.

Rahman, Z. (2016, November 21). Dangerous Data: the role of data collection in genocides Retrieved November 28, 2018, from https://www.theengineroom.org/dangerous-data-the-role-of-data-collection-in-genocides/

Reiermann, J. & Andersen, T. K. (2018). Guldgrube af sundhedsdata samler støv (Gold mine of health data collecting dust) Mandag Morgen

Richterich, A. (2018). The Big Data Agenda: Data Ethics and Critical Data Studies. University of Westminster Press doi: https://doi.org/10.16997/book14

Ritzau. (2018). Deling af motionsdata koster kvinde hendes forsikring. Fyns Stiftstidende (Sharing of exercise data costs woman her insurance): https://bit.ly/2NuODgb

Schaldemose, C (2018) Debat: Slæk ikke på datasikkerheden, Løkkegaard (Debate: Do not relax digital security, Mr Løkkegaard) Børsen

Schwab, K. (2017). The Fourth Industrial Revolution. New York: Crown Business.

Shift Technology. (2018). HICFG Selects Shift to Develop New Counter Fraud Database in the UK! Adgang: https://bit.ly/2OStRZA

Shu, L. L., Mazar, N., Gino, F., Ariely, D. & Bazerman, M H (2012) Signing at the beginning makes ethics salient and decreases dishonest self-reports in comparison to signing at the end Proceedings of the National Academy of Sciences, 109(38):15197200 doi: https://doi.org/10.1073/pnas.1209746109

Sinha, S. (2017). How insurance firms are dealing with fraud claims: https://bit.ly/2xNmzzV

Stensdal, K (2018) Debat om dataetik: Mulighederne med dataanalyser er næsten uendelige – så hvor skal grænsen gå? (Debate on digital ethics: The possibilities of digital analysis are almost endless – so where do we draw the line?): https://bit.ly/2zYf9uV

Thaler, R. H., & Sunstein, C. R. (2009). Nudge: Improving Decisions About Health, Wealth, and Happiness (Revised & Expanded edition). New York: Penguin Books.

Tofte, U (2018) Ulla Tofte: Historien viser, at registrering af data er til vores eget bedste (History teaches us that registration is for our own good) Politiken

Tranberg, P. & Hasselbalch, G. (2016). Dataetik – den nye konkurrencefordel(Digital ethics – the new competitive advantage). PubliShare.

Wagner, B (2018) Ethics as an Escape from Regulation: From ethics washing to ethics shopping? In H. Hildebrandt (Ed.), Being Profiling. Cogitas ergo sum. Amsterdam University Press.

The authors and their commission

This report was written on the commission of Insurance & Pension Denmark with a view to analysing and defining the first important steps towards a common digital ethics for the industry. The purpose is to define a number of principles of digital ethics that not only reflect the opportunities and challenges of data use we see today, but also look ahead towards the scenarios that may acquire great importance in the digital economy and the opportunities of the industry.

The report is based on interviews with representatives of the insurance and pensions industry, external experts and insights from the annual meeting of Insurance & Pension Denmark on 15 November, 2018, on the theme of digital ethics. The report is based on existing expert knowledge in the team and a comprehensive overview of digital ethics. The report was prepared by the consultancy firm Nextwork and written by the following authors:

Brian Due, Ph.D., partner in Nextwork, Head of Research and Innovation and associate professor, Center for Interaction Research and Communication Design, Copenhagen University Expert of digital transformation, innovation and business development. Carries out research in social interaction among employees and the encounter between human being and machine, and advises on knowledge-intensive change processes.

Jesper Højberg Christensen, partner in Nextwork, adjunct professor at CBS, entrepreneur and chairman of the board of directors. Leading expert in strategic communication, branding and business development, organizational change and complicated management processes. Adviser to boards of directors of many large private and public Danish enterprises.

Mads Hennelund, M.Sc., consultant at Nextwork. Advises on digital transformations and organisational change in the digital economy. Expert of strategy, branding and digital ethics and the opportunities and challenges of business development in the financial sector.