14 The uncertain element

Personal data in behavioural insurance

Maiju Tanninen, Turo-Kimmo Lehtonen, and Minna Ruckenstein

Introduction

The expectation that Big Data and Insurtech could disrupt the insurance industry has gained popularity in recent years. Insurance companies all over the world are experimenting with auto, health, and life insurance products that aim to utilise policyholders' behavioural data for various purposes, including product and price personalisation, marketing, and possibly even risk calculations (Cevolini & Esposito 2020; Jeanningros & McFall 2020; McFall 2019; Meyers 2018). These developments fall under the phenomenon of datafication, which suggests 'taking all aspects of life and turning them into data' (Mayer-Schönberger & Cukier 2013, p. 35). Today, data is everything in life that can be digitally traced: from steps, friendships, and driving habits, to breathing, purchases, and daily movements. Digital data's potential for economic value creation lies in its circulation and ability to create relations; data becomes 'lively' (Lupton 2016) in activated market relations. Thus, valuable data is potentially everywhere, but it is more uncertain in that it is 'messier' than before; it cannot be handled and confined to certain predefined uses in the same ordered way as before.

Many of the envisioned disruptive qualities of data, such as personalised pricing and individualised risk profiling, are not and will probably never be feasible because they are subject to strict regulation and contradict some of the basic mechanisms of insurance (Barry & Charpentier 2020; McFall 2019; Tanninen 2020). Yet, the potential to utilise 'messy' and 'lively' data about 'everything' (Thrift 2011) does open new prospects for insurance companies, especially regarding the insurer–insuree relationship. With behavioural data, insurers gain a new kind of access to people's lives which could allow them to develop more selective and close-knit customer relationships (Tanninen et al. 2021).

In this chapter, we look at these (potential) developments from the consumers' point of view and analyse how they experience behaviour-based life insurance products' attempts to create new kinds of data relationships. Our findings highlight the hesitation, confusion and doubt that people have towards the data practices included in the new policies. They also showcase

how the notice-and-consent model, utilised, for instance, in the General Data Protection Regulation (GDPR) enforced in the European Union, is an inadequate means to ensure trustworthy data practices.

Experimenting with digital data requires insurers to leave what appeared to be the ordered world of 'pure' and insulated statistical information in which they are comfortable operating. Although insurance has never been only about statistical data and actuarial calculations (Ericson & Doyle 2004; McFall 2014; O'Malley & Roberts 2014; Van Hoyweghen 2007), the ability to amass and use longitudinal data sets has been a self-evident characteristic of insurance companies to the degree that these operations have been normalised. Data has been defined by certainty in the sense that its uses and movements have been strictly regulated and predictable. However, with the new operations, insurers face novel uncertainties that involve regulatory instability and data existing 'in the wild' because it flows in the 'real world.' Before they can wholeheartedly embrace these new developments, insurers need to experiment with the promise they offer. Even if the data cannot be fitted into neat actuarial categories and statistical analyses, it is seen as a potential new tool and resource, whose value lies in correlations, probabilities, and predictions. Furthermore, it is hoped that digitally tracing what people do will give insurance companies visibility into their lives and offer the possibility to gently manipulate or 'nudge' (Thaler & Sunstein 2009) customers' everyday behaviour in a direction that would be more cost-efficient for insurers in the long term.

As we will demonstrate, however, all this requires that the new practices are seen as valuable and trustworthy by policyholders. If entering the messy realm of digital data is a leap of faith for insurance companies, it is equally so for their customers. Paradoxically, although insurance is intended to provide security and mitigate risk, it can create new anxieties and uncertainties for the consumers (Booth & Harwood 2016). Insurance is an opaque technology to begin with, and the actual trade-offs of a given contract are difficult to estimate. Behaviour-based insurance further complicates the insurer–policyholder relationship, as activity data collected by smartwatches and smartphones and lifestyle interventions aim to gently push people towards healthier and safer habits. In other words, even if people's daily lives are already permeated by messy data practices in the realms of digital services, retail, and social media, creating new kinds of relationships with an entity like an insurance firm is far from straightforward.

To shine a light on how existing and potential policyholders see insurers' attempts to form relationships with them through personalised data collection, we analyse issues raised by data use through a case study of two Finnish behaviour-based life insurance policies. Our main aim is to discuss the uncertainties related to data practices. These uncertainties, we argue, are fundamental to understanding the contextual nature of datafication processes. Obtaining value out of digitalisation requires that data flows can be secured; people need to trust that the operations will benefit

them. For insurers, trust is a requirement for transactions, which are usually understood as an assumed aspect of the customer relationship. Our research suggests, however, that rather than being a given, trust needs to be continuously performed, situated, and embedded in everyday practices (Lobo-Guerrero 2013; Tranter & Booth 2019). In the context of behavioural insurance, it is particularly contested, as customers evaluate the degrees of trust and the overall dependability of data practices; mistrust towards the overall data ecosystem could affect the insurance policies' perceived reliability (Steedman et al. 2020).

Behaviour-based insurance is voluntary and competes with regular products in the private insurance market. Thus, consumers can choose whether to purchase a behavioural policy and submit themselves to data collection. Unlike in the world of social media, for instance, where people have entered into firm data relations, in the realm of insurance they are still considering the harms and benefits of a possible data relationship now and in the future. As Langdon Winner (1980, p. 127) argues, 'the greatest latitude of choice exists the very first time a particular instrument, system, or technique is introduced.' Below, we demonstrate the ongoing negotiations that people participate in to make sense of the data relationship with the insurance company, as it has not (yet) become intertwined with their lives; it is still easier for most people to hesitate and refuse to give up their data.

In the following sections, we first introduce our research site and methodology. Then we discuss our findings in three sections: firstly, we analyse customers' reasons for adopting and using a behaviour-based policy. Secondly, we look at how people make sense of the policies' trade-offs and what makes a 'good deal.' Finally, we discuss the doubt, hesitation, and uncertainty that new policies raise. We conclude by arguing that uncertainties related to the behavioural policies' data practices undermine their trustworthiness. Insurers, thus, need to deal with this uncertainty if they want to include 'lively' digital data in their operations.

Research methodology

Research site and focus

Our case study examines two Finnish behaviour-based life insurance policies, introduced to the market in the latter part of the 2010s by insurers we anonymise as Company X and Company Z. In Finland, citizens are provided universal health care at a very low cost and, if exposed to economic vulnerability, a decent basic income. Thus, private health and life insurance policies are often seen as a form of 'extra security' that 'supplement' the structures provided by the welfare state (Lehtonen 2014; Lehtonen & Liukko 2010). The Finnish insurance market is highly regulated as national laws, the Finnish Financial Supervisory Authority (FIN-FSA), and EU directives set limits for industry operations. Especially the GDPR restricts

insurance companies' experimentations with behaviour-based personalisation in insurance (Thouvenin et al. 2019). Still, the GDPR has faced criticism for its ability to govern the current developments in the field of digital health (Marelli et al. 2020).

The new products by Company X and Company Z combine regular life insurance policies with 'smart' features, including activity tracking conducted with wristbands, smartwatches, or smartphones and eHealth services, such as online health questionnaires and coaching programmes designed by partnering companies. Data tracking is not (yet) deeply integrated into these types of insurance product or the practices of risk pooling, underwriting, and pricing. Instead, insurers frame the new services as additional benefits. For both Company X and Company Z, the policies serve as a response to recent developments, as they experiment with digital data in order to develop more engaging and personalised insurance products. At the time of the interviews, the policies of each company differed in approach. While Company X concentrated more on making available access to eHealth services and did not have an operational reward structure, such as providing premium discounts or cashbacks for active customers, Company Z's policy highlighted financial incentives: it offered its customers bonuses on their insurance coverage if they earned enough 'activity points' to fulfil certain policy requirements.

The behavioural data collected and used in the policies is generated either by tracking devices, such as activity wristbands and smart watches, or by smartphones. In both products, the data is then circulated through a health analytics company that 'purifies' the information of excessive details and glitches and selects certain variables for the insurers' use; the latter seek to collect enough data to fulfil the policies' purposes and comply with insurance regulations. By partnering with analytics companies and eHealth providers, the insurers position themselves as platforms for wellbeing services (Tanninen et al. 2021). The platform structure, however, constitutes a complex network of data relations.

Method and analysis

The empirical materials used for this article consist of 11 focus group discussions that Maiju Tanninen (MT) conducted with actual and potential customers of behaviour-based life insurance products in autumn 2017 and spring 2019. Each focus group had two to eight participants, and overall comprised 46 customers and potential customers, 24 women, and 22 men, ranging in age from their late twenties to their sixties. The discussions spanned from 45 to 90 minutes and were recorded and transcribed.

The policy customers included both people who had already held a behaviour-based policy for some time and individuals who had only recently obtained one. In addition, some informants only had a regular life insurance policy, either because they had not chosen the smart features or they had

not started to use them. In fact, some of our informants had purchased a behaviour-based policy but did not remember this before being reminded of it in the focus group. Finally, MT also interviewed people who did not have life insurance policies from the companies but were seen as potential customers by the market research panels through which they were recruited. This group of informants acted as a comparison group for the insurance clients.

The data was collected in collaboration with the insurance companies as part of a larger research project. We promised to report customer insights that emerged in the focus groups to the insurance companies in order to obtain access to the field, and, especially, establish contact with policyholders, a group that is otherwise difficult, if not impossible, to reach. Because of legal restrictions, we were not allowed to recruit the customers ourselves. Instead, they were contacted by the insurance companies. This could have been a problem in terms of our results' validity if the insurers had determined the 'right' informants for us. However, as recruitment proved to be difficult, the selection of participants ended up being quite random.

The collaborative research design required MT to balance the roles of independent scholar and collaborator. For instance, she needed to emphasise in the focus groups that she did not represent the insurance company. This was generally clear to the customers, but on a few occasions, MT was still addressed as a company representative.

The preliminary analysis of the transcribed focus group discussions was conducted by MT. With the help of automated coding, MT searched for extracts which entailed the concept 'data.' After this phase of research was complete, MT carefully read the interviews and checked the selected extracts, adding or removing excerpts when needed. The selected extracts were imported into an Excel spreadsheet which MT used to conduct more precise thematic coding by hand. Through reading, comparing, and rereading, MT classified the extracts into different thematic categories that represented experiences with personal data and behaviour-based insurance. These codes included 'interest,' 'suspicion,' 'imaginary,' 'privacy,' 'reliability/ trust,' and 'user experience.' This coded data was discussed and analysed by the authors in a joint data session. The initial analysis was drafted by MT based on the data session outcomes, and the final analysis was developed jointly by all authors through rounds of writing and rewriting.

Findings

Adopting the policy

Although behaviour-based insurance policies have previously been discussed in a variety of studies (for a review, see Tanninen 2020), these have typically overlooked the policyholder's perspective. Specifically, why do people opt into these new policies and make the crucial choice of purchasing the technology? In our focus groups, people answered this question

by talking about how the policy appeared to offer something interesting enough for them to acquire, though multiple reasons were provided. Tech-savvy customers were simply keen on trying out the policy, curious about its mechanisms and eager to see its future developments. Others were attracted by the self-tracking features, which they envisioned would help them understand and manage their daily routines, such as sleeping and exercise. Many informants found the policies' (potential) bonuses compelling, providing them with an opportunity to obtain extra coverage or other benefits.

Still, notwithstanding the novel features on offer, the need for insurance remained the main reason for purchasing a life insurance policy, including one with behaviour-based features. Acquiring new kinds of information on one's own life and the possibility of using self-tracking technology were seen as additional benefits, not something essential. What mattered most was the security that insurance offers. However, the 'smart' features appear to have sparked interest and affected the final decision to purchase a policy from a specific insurance provider and thus, in some cases, those features served primarily as marketing devices (see McFall 2014).

In the focus groups, a positive attitude towards and curiosity about the policies were mixed with reservations. The pronounced ambivalence should not have come as a surprise, even for Finnish insurance companies. In fact, their own market research, which was made available to us as researchers, had shown that people are generally quite apprehensive about behaviour-based life insurance products. Though people had voluntarily taken out policies, their outlook was not solely positive. Even if the informants were interested in the products and thought that they were beneficial, they remained fearful and even suspicious about the effect that the new instruments could have on policyholder privacy and on their relationship with their insurance company. Notions of smart insurance appeared to be characterised by more general 'data anxiety' (Pink, Lanzeni & Horst 2018) or 'data ambivalence' (Lomborg et al. 2020).

In the sections below, we discuss in greater detail how the customers speculated about the use of personal data in behaviour-based life insurance policies and reconciled their positive and negative feelings. The oscillation between attraction and concern is not only a characteristic of the insurer–insuree relationship but has also been documented in other kinds of data relations. In all cases, the key question has to do with boundaries: when does 'dataveillance' become too intrusive and creepy (Lupton & Michael 2017; Ruckenstein & Granroth 2020)? The informants see personal data as an asset on which they can capitalise to obtain better services and benefits. As they have chosen to purchase behaviour-based insurance voluntarily, they accept data collection. Yet, they are left with mixed feelings. People were by and large not suspicious of the precise policy that they had taken out or the company that sold it, and they generally thought that they retained their self-determination as to the degree of disclosure of their private daily routines and actions. Still, they did fear a loss of control over their personal

information and struggled to make sense of the complex data relationships that these policies create.

Bargaining data

The financial incentives and rewards incorporated into behaviour-based life insurance were in principle attractive to the customers. They compared the behaviour-based instrument to car insurance products that reward accident-free policyholders with bonuses. The smart policy was seen as a similar mechanism that compensates people for staying healthy. Most of the customers that participated in the focus groups considered these reward structures to be fair. This is in part because the companies do not, at least openly, punish unhealthy or inactive policyholders. Instead, all customers retain their basic level of coverage (or premiums) and can gain bonuses (or discounts).

However, due to their experiences with the tracking devices, some customers doubted whether the self-tracked data was reliable enough for assessing activity levels and determining rewards. The inaccuracies and deficiencies of such data are widely known (Gorm & Shklovski 2019; Pink et al. 2018), and our informants also reflected on the devices' inability to measure their activities correctly; the data did not resemble their 'real selves' (Lupton 2020). Thus, even though people did not oppose the policies' rewarding structures per se, they had concerns with the trustworthiness of the behavioural data. Two of Company Y's customers, Teemu, an IT professional in his late 30s and Anne, a sales manager in her 40s expressed their concerns as follows:

TEEMU: But how they are going to measure it [health]; that is the tricky question. What data is it based on?
ANNE: Yeah, that should truly be something trustworthy. It cannot be merely the device: it's not enough.
TEEMU: Yes, it can't remain open to interpretation.

Unlike car insurance, where eligibility for bonuses is checked annually, in smart insurance the idea is that policyholders' risk scores could be assessed and determined based on real-time data (Meyers & Van Hoyweghen 2020; Zuboff 2019). However, at least in our case study, this idea appears to be unfeasible in life insurance due to both consumer objections and technological and regulatory limitations (Tanninen 2020; Tanninen et al. 2020). Many of our informants recognised that the usefulness of behavioural data stems from longer time series such as monthly averages. This was also the approach in Company Z's policy, which rewarded its customers based on their average score over a period of several months. As the final estimation was based on this longer time frame, policyholders appeared more accepting of small inaccuracies in their data.

Still, people did not deem it enough to be rewarded only after reaching the goals specified in policies. Instead, the focus groups revealed that, despite any inaccuracies, people's personal data has innate value regardless of their activity status, and a policy's terms and conditions should be attractive enough for them to give out their personal information. Clearly, people can regard their data as a form of currency with meaningful purchasing power, echoing demands made by technology developers to combat informational asymmetries. For instance, Lanier (2013) argues that as commercial agents profit from digital traces, a portion of their gains should be distributed to the data subjects as remuneration for providing their data. This view resonated with how Matti, a paramedic in his 40s, approached the matter.

> I don't think people like the idea of being monitored, or, at least, I don't like it. But if you got some support and guidance for, say, exercising – or could there be a discount for the gym, a personal trainer or dietician services [included in the policy]? I don't like the idea that in return for being stalked and monitored and being subjected to data collection and data distribution, I would get just a [premium] discount.

In the focus groups, people not only assessed existing practices but also went further. They began to imagine 'good' and 'bad' deals with insurance companies and to think about their own bargaining power. For instance, Marjo, a 45-year-old university lecturer who did not yet have a behaviour-based policy said that she 'could maybe take the smart features as a freebie if the insurance price remained the same.' Another interviewee, Eero, a chef in his 50s reflected that if he 'got a great deal with some [wellbeing] service provider,' he might allow the insurance company to gather his data. Thus, customers expected something in return for their personal data, even when they were *not* conforming to the activity or health goals set by the policies.

An especially striking finding in the interviews was that, in a world of digital services, consumers appear to value especially highly connection with, and help from real-life experts. As Matti's statement above exemplifies, people were interested in receiving guidance from medical professionals, dieticians, and personal trainers who could help them interpret their data and plan health interventions based on it. Only on some occasions did customers feel that it would be sufficient to have their data interpreted by a robot or an artificial intelligence application – a finding that must be a disappointment, considering the insurance companies' ambitions for the data economy of the near future (Grundstrom 2020). Instead of a novel, largely automated circulation of information that would enable cutting labour costs for insurance companies, our focus groups appear to imagine that the new data circuits will create more personalised services based on *human* interpretation and interaction.

The fairness of the (current) trade-offs between the data, rewards, and services was reasoned about in varying ways. Some felt that the exchange

was fair, as they could get an increase in their insurance coverage or use the eHealth services attached to their policies. Others did not find the trade-off appealing enough, especially when it comes to financial rewards. This was discussed by Ossi, a customer service agent in his 30s and Hanna, a project manager in her 40s.

OSSI: A discount of five euros per year? That won't do it.
HANNA: I would just be wondering if I am selling my soul for five euros.

Obviously, small rewards neither motivate people to pursue policy goals nor compensate them for the collection of their data. Furthermore, the reference to selling one's soul for five euros vividly highlights the depth of apprehension and mistrust that people can have towards data collection. For Hanna, the actual trade-off is not clear. Will she be selling her soul to the insurance company for a relative pittance and signing up for something that might harm her?

Along with the modest financial rewards, some customers also criticised the services included in the policies. Mikko, an engineer in his 40s, said, 'the data collection is totally fine by me, but they should use it and loop it back to me so that I could get something concrete in return.' Here, the issue is not so much the mistrust placed in the data collection but the lack of a proper 'feedback loop' (Ruckenstein & Pantzar 2017) to build actionable insights with the data. As the services were not seen as advanced or tailored enough, the companies' promises of personalisation remain unfulfilled. One of the core promises of the data economy fails if the new information that is disseminated does not reach the customer in a meaningful way. Thus, instead of truly personalising prices or services, the 'smart' features only appear to help companies stand out from their competitors at the point of sale (McFall 2019; McFall & Moor 2018). Partly because of their lack-lustre experiences, a number of our informants had stopped using the policies' behaviour-based features or used them only in a desultory, unengaged way. Hence, customers were dropping out of the schemes and becoming traditional life insurance clients or, in some cases, the collection was still occurring through the mobile app without the customers' active participation or interest.

Data doubt

As the thoughts about room for bargaining above demonstrate, ideally, people want to be able to control the insurer–insuree relationship and set limits on the smart policies. The informants hoped the trade-off would be beneficial: they required something in return for their data, and some opted out of the behaviour-based services if these were not sufficiently engaging. Furthermore, they found it important to retain a sense of autonomy and feel that they *chose* the forms in which their data is tracked. Kaisa, a HR

specialist in her 40s, discusses personal choice as a precondition for the decision to adopt the technology. Acknowledging the fact that she had agreed to data collection, she thinks that 'it's OK.' Yet, 'in a broader perspective,' she does not view such practices as 'a good idea,' especially if it would be 'mandatory and compulsory.' That would be too 'controlling' and too 'top-down.' More generally, our informants tended to underline the importance of smart policies and data tracking being voluntary: the data collection and 'nudging' policy features were considered acceptable if they were chosen by the policyholders.

Although people might accept the current state of a policy that they had taken out, similarly to Kaisa's case above, they feel unease regarding the smart policies' abilities and potential effects. Those possible negative effects were the subject of speculation in the focus groups, sometimes with humorous and exaggerated overtones. For instance, informants shared vivid visions of insurance companies' monitoring their behaviours, movements, and similar parameters in real time, essentially becoming unwelcome guests or even stalkers. In these exaggerated narratives, insurers would interrupt everyday situations ranging from relaxing on the sofa to having a night out by giving not only unsolicited (health) advice but also direct commands, scolding, and physically forcing the customers to return to healthy habits.

Yet, importantly, the customers were not certain which of the forms of surveillance were actually already taking place and which were only imaginary. The limits of data collection were unclear. For instance, people did not know whether the insurers received their location information and generally lacked specific knowledge of what data was being collected. This uncertainty is attested by Antti, a bank clerk in his 30s:

> Now I am not really sure which data is going there [to the insurance company]; I have just accepted that the information is transferred and which info is included. Are they [the insurance company] using just the data on the activity points? Is that enough for them, or are they receiving something else as well?

As Antti's example shows, uncertainty can exist and persist even when customers have signed an insurance contract and accepted its data policy. This doubt might be related to the policies' platform structure, as the mediation provided by the data aggregator companies and eHealth service providers complicates the data relationship. All these service providers have their own data policies for customers to accept, which makes it hard for them to keep track of who is collecting what data and all the purposes for which it is being used (Draper & Turow 2019).

The interviews made it clear that customers want to feel certain that, even if the insurance companies control the data, they would not accidentally disclose it for inappropriate uses. Despite the uncertainty related to the

question of what data is being collected, the interviewees generally thought that insurance companies are trustworthy custodians of data since they have a long history of dealing with sensitive information. Still, they thought that digital data has an inherent uncertainty and is prone to security breaches (Pink, Lanzeni & Horst 2018). In a way, digital data and its movements were seen as uncontrollable, which could lead to unwelcome surprises.

For instance, the interviewees discussed the possibility that hackers could steal their data and use it for criminal purposes. They also speculated how corporate acquisitions could make their data become much more widely available than was originally intended. Moreover, people imagined how their data could come to haunt them in unexpected contexts, such as targeted advertisements, which many customers used as a reference point to make sense of the data's possible movements. Targeted advertising is something that people experience in their everyday lives: their clicks, choices, and purchases are looped back to them, sometimes creating good matches but other times resulting in annoying and even creepy encounters (Ruckenstein & Granroth 2020). Advertising is a concrete example of how personal data can be used for commercial purposes, perhaps without people being aware of it. The movements of data are just as undesirable; in the worst cases, they violate policyholders' sense of intimacy and self-determination.

Conclusion

Our study highlights the data ambivalence that is prevalent in customers' relationships with behaviour-based insurance policies and the practices those policies support. The informants were curious and interested in the products and perceived voluntary self-tracking practices not only as acceptable but also as positive. Yet, their sense of self-determination was undermined, to varying degrees, by the fact that they were not certain of what kind of data was being collected and to whom it was being made available. The analysis shows that the ambivalence extends beyond the immediate relations between people and their personal information. Uncertainties, anxieties, and apprehensions are associated with insurance, and the data economy at large, and the relationships embedded within these. Where will the data travel? Will it change the insurance terms and conditions? Will it harm me in the future?

These uncertainties undermine the policies' trustworthiness. Although people often regard self-tracked data as non-personal 'background noise' (Ajana 2020), they express concern about data movements and leakages. Our case study highlights a generalised confusion regarding what information is being collected and by whom. In practice, privacy policies are difficult to understand – even for people working in that field – and it is clearly a lot (too much) to ask people to familiarise themselves with details involved in all of their data relationships. The lack of awareness and confusion exemplifies the limitations of the notice-and-consent model used, for instance, in

the General Data Protection Regulation enforced in the European Union. In light of our study, the model is inadequate in ensuring trustworthy practices, as it fails to consider people's everyday realities and hesitation when engaging with the policies (see also Marelli et al. 2020).

The customers' lack of knowledge is also related to questions of information asymmetry. The processes of datafication are built on informational asymmetries, but in the insurance context the concept usually refers to customers withholding information that is crucial for underwriting, thus increasing risk for adverse selection, that is, the disproportioned selection of high-risk individual in the pool (Baker 2003; McGleenan 1999). Social scientists have, however, pointed out that the asymmetry works the other way around, as well: insurers have much more information about a given instrument and the associated population values and averages than the customer (Van Hoyweghen 2007). Behaviour-based life insurance policies are no exception. We have demonstrated how customers struggle to make sense of the wider context of the policies and how they lack certainty on precisely what they are signing up for. Thus, the information asymmetry places policyholders in a vulnerable position, as it is very difficult for them to reliably estimate the policies' possible effects. At present, this unequal arrangement might be partly related to the policies' experimental nature; even the insurers themselves do not know what will become of the new operations and thus cannot communicate it clearly to customers (Jeanningros 2020; Meyers & Van Hoyweghen 2020; Tanninen et al. 2020).

Thus, what is at stake with uncertain data for both the insurance companies and in the data practices is how trust will be maintained or created under these new conditions. The interviewees wanted to feel secure that even if insurers (or the information technology and wellness companies that mediate the insurance practice) controlled their data, they could obtain a reasonable reward for that fact. Yet, such a transactional logic does not in and of itself guarantee trustful relations. It was hard for people to evaluate what the price of their behavioural data should be. Furthermore, customers wanted to be sure that the data would not be used for inappropriate uses such as online crime or questionable commercial practices and found it difficult to assess who to trust.

Our case speaks to the need for a careful building of trust as the insurance industry moves onto the terrain of the emerging data economy. The data relationships that insurers promote need careful planning and following through to become genuinely trustworthy. Otherwise, the industry faces the risk of raising a new kind of mistrust in people, evidence of which we can already see in the empirical material presented here. We have demonstrated how people find it difficult – if not impossible – to assess how to trust insurance, especially in the long run. If digital data is an uncertain, lively, and messy element, the insurers need to make sure that they can handle that uncertainty. Otherwise, the insurance industry as we have known it will no longer be viewed as capable of responsibly managing sensitive personal information.

References

Ajana, B 2020, 'Personal metrics: Users' experiences and perceptions of self-tracking practices and data', *Social Science Information*, vol. 59, no. 4, pp. 654–678.

Baker, T 2003, Containing the promise of insurance: Adverse selection and risk classification, In Ericson, R.V & Doyle, A (eds), *Risk and Morality*, Toronto: University of Toronto Press.

Barry, L & Charpentier, A 2020, 'Personalization as a promise: Can Big Data change the practice of insurance?', *Big Data & Society*, vol. 7, no. 1, <https://doi.org/10.1177/2053951720935143>.

Booth, K & Harwood, A 2016, 'Insurance as catastrophe: A geography of house and contents insurance in bushfire-prone places', *Geoforum*, vol. 69, pp. 44–52.

Cevolini, A & Esposito, E 2020, 'From pool to profile: Social consequences of algorithmic prediction in insurance', *Big Data and Society*, vol. 7, no. 2, <https://doi.org/10.1177/2053951720939228>.

Draper, N.A & Turow, J 2019, 'The corporate cultivation of digital resignation', *New Media & Society*, vol. 21, no. 8, pp. 1824–1839.

Ericson, R.V & Doyle, A 2004, *Uncertain business: risk, insurance, and the limits of knowledge*. Toronto: University of Toronto Press.

Gorm, N & Shklovski, I 2019, 'Episodic use: Practices of care in self-tracking', *New Media & Society*, vol. 21, no. 11–12, pp. 2505–2521.

Grundstrom, C 2020, 'Health data as enabler of digital transformation. A single holistic case study of connected insurance', PhD Thesis, University of Oulu.

Jeanningros, H 2020, 'Conduire numériquement les conduites. Économie comportementale, objets connectés et prévention dans l'assurance privée française', Thèse doctorale, Sorbonne Université.

Jeanningros, H & Mcfall, L 2020, 'The value of sharing: Branding and behaviour in a life and health insurance company', *Big Data and Society*, vol. 7, no. 2, pp. 1–15.

Lanier, J 2013, *Who owns the future?* USA: Simon & Schuster.

Lehtonen, T.K 2014, 'Picturing how life insurance matters', *Journal of Cultural Economy*, vol. 7, no. 3, pp. 308–333.

Lehtonen, T.K & Liukko, J 2010, 'Justifications for commodified security: The promotion of private life insurance in Finland 1945–90', *Acta Sociologica*, vol. 53, no. 4, pp. 371–386.

Lobo-Guerrero, L 2013, 'Uberrima Fides, Foucault and the security of uncertainty', *International Journal for the Semiotics of Law*, vol. 26, no. 1, pp. 23–37.

Lomborg, S, Langstrup, H & Andersen, T.O 2020, 'Interpretation as luxury: Heart patients living with data doubt, hope, and anxiety', *Big Data & Society*, vol. 7, no. 1, pp. 1–15.

Lupton, D 2016, *The quantified self: A sociology of self-tracking*, Cambridge, UK: Polity Press.

Lupton, D 2020, ''Not the Real Me': Social imaginaries of personal data profiling', *Cultural Sociology*, vol. 15, no. 1, pp. 3–21.

Lupton, D & Michael, M 2017, ''Depends on who's got the data': Public understandings of personal digital dataveillance', *Surveillance & Society*, vol. 15, no. 2, pp. 254–268.

McFall, L 2014, *Devising consumption: Cultural economies of insurance credit and spending*, London: Routledge.

McFall, L 2019, 'Personalizing solidarity? The role of self-tracking in health insurance pricing', *Economy and Society*, vol. 48, no. 1, pp. 52–76.

McFall, L & Moor, L 2018, 'Who, or what, is insurtech personalizing? Persons, prices and the historical classifications of risk', *Distinktion: Journal of Social Theory*, vol. 19, no. 2, pp. 192–213.

McGleenan, T 1999, Genetic testing and the insurance industry, In McGleenan, T, Wiesing, U & Ewald, F (eds), *Genetics and insurance*, Oxford: BIOS Scientific Publishers Limited.

Marelli, L, Lievevrouw, E & Van Hoyweghen, I 2020, 'Fit for purpose? The GDPR and the governance of European digital health', *Policy Studies*, vol. 41, no. 5, pp. 447–467.

Mayer-Schönberger, V & Cukier, K 2013, *Big Data: A revolution that will transform how we live, work and think*, London: John Murray.

Meyers, G 2018, 'Behaviour-based personalisation in health insurance: A sociology of a not-yet market', PhD Thesis, KU Leuven.

Meyers, G & Van Hoyweghen, I 2020 "Happy failures': Experimentation with behaviour-based personalisation in car insurance', *Big Data & Society*, vol. 7, no. 2, pp. 1–14.

O'Malley, P & Roberts, A 2014, Governmental conditions for the economization of uncertainty, *Journal of Cultural Economy*, 7, no. 3, 253–272, DOI: 10.1080/17530350.2013.860390

Pink, S et al, 2018, Broken data: Conceptualising data in an emerging world, *Big Data & Society*, vol. 5, no. 1, pp. 1–13.

Pink, S, Lanzeni, D & Horst, H 2018, 'Data anxieties: Finding trust in everyday digital mess, *Big Data & Society*, vol. 5, no. 1, pp. 1–14.

Ruckenstein, M & Granroth, J 2020, 'Algorithms, advertising and the intimacy of surveillance', *Journal of Cultural Economy*, vol. 13, no. 1, pp. 12–24.

Ruckenstein, M & Pantzar, M 2017, 'Beyond the quantified self: Thematic exploration of a dataistic paradigm', *New Media & Society*, vol. 19, no. 3, pp. 401–418.

Steedman, R, Kennedy, H & Jones, R 2020, 'Complex ecologies of trust in data practices and data-driven systems', *Information, Communication & Society*, vol. 23, no. 6, pp. 817–832.

Tanninen, M 2020, 'Contested technology: Social scientific perspectives of behaviour-based insurance', *Big Data & Society*, vol. 7, no. 2, pp. 1–14.

Tanninen, M Lehtonen, T.K & Ruckenstein, M 2021, Tracking lives, forging markets, *Journal of Cultural Economy*, vol. 14, no. 4, pp. 449–463.

Thaler, R & Sunstein, C 2009, *Nudge: Improving decisions about health, wealth and happiness*, London: Penguin Books.

Thouvenin, F, Suter, F, George, D et al. 2019, 'Big data in the insurance industry: Leeway and limits for individualising insurance contracts', *JIPITEC*, vol. 10, no. 29, pp. 209–243.

Thrift, N 2011, 'Lifeworld Inc—and what to do about it', *Environment and Planning D: Society and Space*, vol. 29, no. 1, pp. 5–26.

Tranter, B & Booth, K 2019, 'Geographies of trust: Socio-spatial variegations of trust in insurance', *Geoforum*, vol. 107, pp. 199–206.

Van Hoyweghen, I 2007, *Risks in the making: Travels in life insurance and genetics*, Amsterdam: Amsterdam University Press.

Winner, L 1980, 'Do artifacts have politics?', *Daedalus*, vol. 109, no. 1, pp. 121–136.

Zuboff, S 2019, *The age of surveillance capitalism: The fight for a human future at the new frontier of power*, New York: Public Affairs.