Check for updates

JITTC

Teaching Case

Big data and data ownership rights: The case of car insurance

Journal of Information Technology Teaching Cases
2023, Vol. 13(1) 82–87
© Association for Information Technology Trust 2022
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/20438869221096859
journals.sagepub.com/home/jittc
SAGE

Tzameret H Rubin[1], Tor Helge Aas[2] and Jackie Williams[3]

Abstract

Customers' data points sources are growing, through the Internet of Things (IoT), telematics and interfacing with third parties' platforms. Third parties provide either by-product data about their clients, or data that are generated for the specific task of a more accurate measurement of behaviour. One of the core building blocks in insurance is understanding risk – therefore, innovation around data points (sources and analytics) to proxy risk is the engine behind its digital transformation. While the value of data points is clear for the providers of insurance products and services, the customers have not only less control over their data, but also hardly benefit from the creation of those data points. In this paper we provide a case study from the British car insurance industry, about a data-driven product that pivoted into a re-designed personal data right architecture, which included transparency, traceability and usability of customers' digital traces, and enabled customers' ownership rights over their data.

Keywords

Data ownership rights, insurtech, digital transformation, big data

Introduction

Big Data is at the heart of the digital transformation in the insurance industry (Fang et al., 2016). It improves administration and speeds up claims and settlements, and it allows training of backbone algorithms that are the core of Machine Learning (ML) and Artificial Intelligence (AI) models that are improving products, services and processes.

As insurance companies adapt to use Big Data, considerations related to privacy-utility trade-offs of data (Abowd and Schmutte, 2019) and Data Ownership Rights (DOR) arise. As data emerges and flows through different channels, such rights become more ambiguous and users become more vulnerable to unfair and illegal practices, or their personal data being unknowingly exploited (Burrell, 2016).

These considerations impact the insurance sector. Whilst both data and technology remain pivotal to the insurance industry, it is questionable whether the established services architecture will, or is able to, provide services with transparency, traceability and usability of customers' digital traces, in order to allow individuals to have DOR over their data (Ng, 2018).

In this paper, we explore the case of car insurance using social network behavioural data to proxy risk for young drivers. Through this case we address the challenges of data ownership, and discuss the need for 'bootstrapping' the data ownership paradigm, that is, re-thinking the architecture of services and data.

The rest of this paper is structured as follows: We first set the scene by discussing car insurance and the type of data points that are used for credit score in general, and in particular for assessing risk for young drivers. Second, we discuss the Data Ownership concept and its application within insurance services. Thereafter, we provide the story of a startup called Visual DNA that developed a novel risk score and personalised data business proposition for young drivers, for Admiral, a car insurance company, which pivoted towards the OneZero-me broader FinTech 'digital wallet' innovation. Lastly, we provide some conclusions and a list of discussion questions.

Car insurance for young drivers

Historically, insurance companies did not differentiate their customers' risk, and provided a unified premium for each

[1]Oxford Brookes Business School, Oxford Brookes University, Oxford, UK
[2]School of Business and Law, University of Agder, Kristiansand, Norway
[3]School of Business and Economics, Loughborough University, Loughborough, UK

Corresponding author:
Tzameret H Rubin, 1Oxford Brookes Business School, Oxford Brookes University, Oxford, UK.
Email: t.rubin@brookes.ac.uk

insurance line. However, over the years, better probabilities models have been implemented by the industry to proxy risk for different type of customers, based on parameters such as age, address, car engine size, security systems or the driver completing additional training courses.

Young drivers are seen as high risk due to the cost and frequency of claims within the 18–25 age group, and insurance cover is priced across the group accordingly (Association of British Insurers, 2021). Premiums could be argued as excessively high, being based upon static data to map risk at the point of application.

To address the issues of high insurance premiums for young drivers there have been major advances. Black box insurance, or telematics, that provides levels of behavioural control via specific driving requirements is a case in point (Zuboff, 2019). The black box uses location and gyroscope technologies that continually tracks driving habits, such as mileage, braking, speed, and day or night use, either via a device fitted to the car or via a smartphone app. First, this enables the collection of real time behavioural data points that can assist the insurer to tailor a more accurate profile of the driver, hence reduce its fixed insurance premium, or even provide usage-based insurance. Second, it provides real time feedback for the driver for correcting more dangerous driving, as a preventative measure (Bell, 2018; Floow, 2020). Third, the gathered data points can also assist analytics tools to train AI models that can create value for the service provider and be a basis to develop new 'future behaviours products' (Zuboff, 2019).

New insurance products can be readily embraced where there is a particular need in the market. However, even when a product is popular it may raise significant concerns within society.

An independent report on behalf of Association of British Insurers, by BritainThinks (2019), highlighted the many issues felt by consumers regarding data collection, particularly by data brokers and how the data would be used by insurance companies. The ability to 'opt out' of providing data was not always apparent, consent being gained by default rather than the consumer proactively selecting to 'opt in'.

This issue relates to a lack of clarity regarding the data 'ecosystem' and how it is seen as an imbalance of power between consumer and industry. Data points are traditionally owned by the service provider, This means that although the data was generated by the drivers, they are not only assisting the service provider train their algorithms, that is, creating value for them, but they do not own their intellectual property on their data; hence, the drivers cannot monetise their data and end up receiving just a fraction of the total value their data generates.

Data ownership rights

Personal data is the footprint of the users' usage of multiple apps, websites and services, and what is coined 'surplus behaviour data', including texts, photos, messages, and purchases (Zuboff, 2019). The importance of personal data ownership became more apparent over the years following the growing value of Big Data (Acquisti, 2010). Personal data ownership is of concern across the service sector, in particular due to information asymmetry between consumers and service providers. From the consumers' perspective, although there is evidence that disclosing personal data may be beneficial to individuals (Akcura et al., 2005), data sharing brings negative externalities such as privacy costs, as a socially agreed value within specific contexts (Acquisti et al., 2015), and damages the perception of privacy, subjectively and objectively (BritainThinks, 2019). From the service providers' perspective, if businesses will not be able to obtain customers' data, due to complete privacy regulation, it can result in loss of opportunity costs and inefficiencies (August and Tunca, 2006; Van Zandt 2004; Hann et al., 2006).

An alternative approach is providing DORs to neither the service providers nor the customers, but instead to a broker entity. This may increase aggregate welfare, emphasising market self-correction for efficiency outcomes, and allow the regulators steering the market through a combination of incentives, disclosure policies and even liability (Acquisti 2010).

However, the use of a broker entity is not flawless. First, Godel et al. (2012) highlighted that many data exchange contracts will cause a lack of transparency for any secondary use of data, in particular when the individual users are not directly involved in the transaction between third parties trade of data (Swire and Litan, 1998). Secondly, when service providers hold the users' data, they hold the intellectual property rights to the data, meaning it might be difficult to differentiate clearly between the corporate data versus the users' personal data (Shapiro and Varian, 1997, 1998). These disadvantages clearly portray the challenge for users to control and own their personal data with the current service providers' architecture (Ng, 2018).

In the following section we cover a story about innovation in car insurance that pivoted into a wider, more fundamental innovation. This story is about a data ownership problem that triggered the re-invention of a business proposition which, instead of creating a new business proposition based on Big Data, it fundamentally changed the balance of value for the insurer and their customers, with a generic Person-Controlled Personal Data (Ng, 2018).

The case of admiral car insurance

Use of data in admiral

Admiral car insurance was established in 1993 as a specialist provider of car insurance. By 2018 Admiral had insured four million cars, covering one in seven cars in the UK. Their products have developed alongside customer

demand and social change and are also representative of the company ethos, offering a simple, hassle-free solution to insurance cover, with convenience and reward being central to their products (Admiral, 2021).

In 2016, Admiral ran a pilot with the vast volumes of data generated via consumers' social media, to indicate certain personality traits linked to safe driving. For example, conscientious individuals could be identified from their use of lists or concise sentence structure in contrast to their over-confident peers with their overt use of exclamation marks and emphatic immediate answers on social media (Ruddick, 2016). However, rather than merely gathering simplified personality indicators, Admiral aimed to challenge the fixed assumptions of what actually denotes a safe driver. Using algorithms developed by their collaborator startup, Visual DNA, to provide correlations between social data, and actual claims data, aimed to allow the technology to constantly evolve based on thousands of combinations to generate risk predictions (Borenstein in Ruddick, 2016).

At a TECHNGI research group and Willis Research Network (WRN) 'AI & Next Gen Insurance Services' conference, held in London (TECHNGI, 2019), the former Chief Data Officer of Visual DNA, explained that the Visual DNA team had suggested that click-stream-data could be used to predict risk as a seamless option. The idea was pitched to Admiral and generated much excitement as it aligned with the company's ethos and had the potential to solve a real problem, that is, to overcome the lack of young drivers' driving history and the inherent inability to correctly assess their risk using behavioural data points, extracted from third-party social platforms, specifically Facebook.

Through Facebook API, Visual DNA collected the pilot participant users' behavioural digital footprint to proxy a risk variable, risk that is translated into premium by Admiral. The link to Facebook users was done with the users' direct consent. The product was fully compliant with FCA and ICO regulations. The proof of concept was defined as a success both for Admiral and for the pilot users that participated in that pre-launch.

However, at the eleventh-hour, Facebook unilaterally decided to withdraw their approval to allow access to their accounts' data, and disable their API for Visual DNA. This has created a challenge as was generally described by Ng (2018):

> ''..re-use and re-sharing of data rights with others, even with individuals' consent, become problemsome for data brokers because the original rights of the data continue to stay within the source. In other words, if a data broker collected Facebook data on an individual's behalf, the data broker would have to abide by Facebook's terms and conditions for re-use and resharing, even if individuals themselves are willing to contract on."

Re-thinking the architecture of services and data in admiral

The pivotal moment for Visual DNA was at the point they realised their product completely relied on the platform companies such as Google, Amazon, Facebook and Apple (GAFA) that hold both services and users' data together. While a user accepts terms and conditions for using a platform service, their data is carefully monitored and creates value for the service providers, but are not owned or benefit the consumers with the immediate service they consume.

This understanding pivoted Visual DNA, to become OneZero-me. Built on previous knowledge OneZero-me's critical addition was the separation of users' data from the service, allowing the consumers to have the control of their own data.

The aim of OneZero-me was to bring greater financial opportunity and inclusion to people who were unable to access key services, as well as to enable more balanced and refined pricing for all. It offers an alternative risk score, such as credit score and motor scores, to improve customer's eligibility access for a range of financial products.

The solution offered by OneZero-me is called 'digital wallet identity'. In their architecture, the data is owned by the end user. For example, if a social network platform would like to share an individual's data with any third party, it will need the 'data wallet owner' consent, to ensure that the 'digital wallet identity' will gain the benefit for sharing or selling the data.

The technology behind 'digital wallet identity'

The decentralised web model that separates data from services can be based on different technologies, either Distributed Ledger Technology (DLT); a piece of software that resides on mobiles; or a Cloud based solution. Both solutions keep privacy and control of users' data, by users, as described in Figure 1, based on Verborgh (2017). The left-hand side of the figure illustrates a traditional service market where the service platforms hold their customers data. Third parties ('innovative competitors' in the figure) that would want to build new products/services on customers' data in this market would need to interface with the platform companies and be granted access to the users' data (with limited fields that the platform company would like to share).

However, on the right-hand side of the figure, the architecture of OneZero-me is illustrated. Here the market is divided into a service market ('app market' in the figure) and a data market. In this architecture, the service providers' platforms have the same hierarchical level as any platform to access users' data, while the users themselves can grant the permission to access their data.

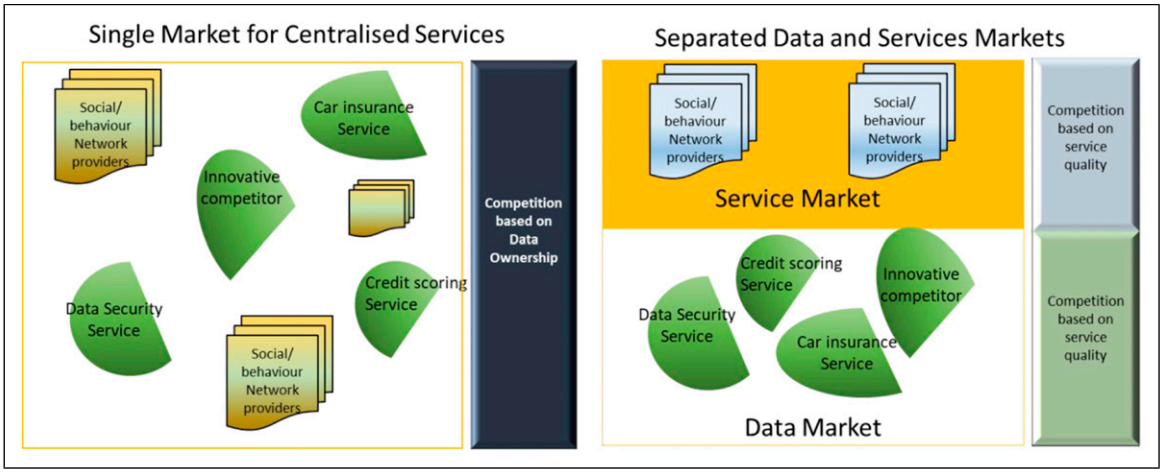

Figure 1. Data and services market structure.

Discussion and conclusions

Being one of the oldest existing industries, insurance in its core is still the same. However, the growing digital transformation pushes this industry's stakeholders, to improve processes, reduce costs in order to provide lower premiums, improve user experience, provide a tailored product or any value creation for the customer. This digital transformation occurs through data-driven solutions that are changing this industry, with the customers at its heart. The case study discussed in this paper reveals a story of a startup that originally developed a data-driven product, based on a third-party source of data, but pivoted into redesigning their business proposition of a new personal data right architecture, not only for the insurance industry but for any financial service provider that requires a bespoke 'risk score' in order to improve inclusivity, transparency and usability of customers' digital traces, in order to allow individuals to have control over their data.

The case of Admiral highlights deeper societal issues, such as concerns regarding collection of personal data and its use. Whilst Facebook had effectively determined the initial Visual DNA solution as non-viable, the issues of fear, mistrust and ethics were clear to see in the media and public response. The perception of a large corporation operating a 'surveillance culture' to gain insights from private media postings was a significant issue, even if the users provided their consent to link their Facebook data with Admiral car insurance.

Specifically, the Visual DNA data-driven product was based on Facebook's API as a third-party data provider, harvesting users' digital appearance on social media and monitoring their behaviour in order to proxy their risk. That risk was piloted to feed into Admiral insurance risk modelling, for tailored car insurance for young drivers, a population group that traditionally pay the highest premium due to a lack of historical individual risk scores. This is a particularly interesting case because this venture hit the wall and 'failed' just before it was launched, due to personal DORs. However, this failure was leverage in order to address a bigger industry problem – personal data ownership. An improved model of data ownership has the potential to stimulate a broader growth for insurTech start-ups that would not need to rely on third party data in order to create new products and services.

Through the case of Admiral this paper provides the image of an industry in transformation, not only through incremental innovation products or services, but on a more generic problem-solving, that technology can assist in addressing and guiding the regulators with a proposed customer-centric solution. Specifically, the newly concept of designing a new data ownership paradigm of separating service from data can disrupt the whole advanced services sector and can be applied for any marketplace that might benefit from independent risk assessment that is within the customers' control.

It is important to note that designing standards that are open and transparent does not directly equate to them being accountable (Ananny and Crawford, 2018). Therefore, there is a need for further innovation to build new architectures, centralised or decentralised, that will differentiate between 'data subjects', that is, data points generated by individuals' usage of a service, and 'data controllers' the service providers (Ramokapane et al., 2021). Even if data subjects are data controllers and processors, as is the case with the HAT architecture and Data swift's personal data accounts, stewardship of data sharing would still be required, as it is with payments and bank accounts.

Questions for discussion

1. How has car insurance risk-measurement evolved over the years in the UK?
2. Can you describe how Telematic, and Behaviour Dynamic Data allow mitigate price discrimination for disadvantaged population such as young drivers?
3. How does a 'digital wallet' work, with respect to customers' usage?

4. What is the role of the regulator with respect to data ownership in the insurance industry?

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Innovate UK and the grant number is ES/S010416/1.

ORCID iD

Tzameret H Rubin https://orcid.org/0000-0001-5390-8600

References

Abowd JM and Schmutte IM (2019). An economic analysis of privacy protection and statistical accuracy as social choices. *American Economic Review*, *109*(1), 171–202.

Ananny M and Crawford K (2018). Seeing without knowing: limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society 20*(3): 973–989. SAGE Publications.

Acquisti A (2010). *The Economics of Personal Data and the Economics of Privacy. Background Paper for OECD Joint WPISP-WPIE Roundtable, 1*.

Acquisti A, Brandimarte L and Loewenstein G (2015). Privacy and human behavior in the age of information. *Science*, *347*(62221), 509–514.

Admiral (2021). *Our Milestones*. [Online]. Available at: https://www.admiral.com/about-us/our-milestones (Accessed 27 April 2021).

Akçura MT and Srinivasan K (2005). Research note: customer intimacy and cross-selling strategy. *Management Science*, *51*(6), 1007–1012.

Association of British Insurers (2021). *Age and Motor Insurance*. [Online]. Available at: https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/motor-insurance/age-and-motor-insurance/ (Accessed 19 April 2021).

August T and Tunca T (2006). Network software security and user incentives. *Management Science*, *52*(11), 1703–1720.

Bell R (2018). *Floow Rewards*. [Online]. Available at: https://www.thefloow.com/latest/rewards-telematics-improvements-driver-behaviour/ (Accessed 17 March 2021).

BritainThinks (2019). *Association of British Insurers (2019). The Price Of Accuracy? Customer Data And Insurance Report 2019*. [Online]. Available at: https://www.abi.org.uk/globalassets/files/publications/public/data/britain_thinks_consumer_data_insurance_report.pdf (Accessed 19 April 2021).

Burrell J (2016). How the machine 'thinks': understanding opacity in machine learning algorithms. *Big Data & Society*, *3*(1), 205395171562251.

Fang K, Jiang Y and Song M (2016). Customer profitability forecasting using big data analytics: a case study of the insurance industry. *Comput. Ind. Eng*, *101*, 554–564.

Floow (2020). *Floowkit* [Online]. Available at: https://www.thefloow.com/our-solutions/floowkit/ (Accessed 18 March 2021).

Hann IH, Hui KL, Tom Lee SY and Png IPL (2007). Overcoming online information privacy concerns: An information processing theory approach. *Journal of Management Information Systems*, *24*, 13–42.

Godel M, Litchfield A and Mantovani I (2012). The value of personal information: evidence from empirical economic studies. *Communications & Strategies*, *88*(4th Quarter), 41–60.

Ng ICL. (2018), '*Can You Own Your Personal Data? the HAT Data Ownership Model', University of Warwick Service Systems Research Group Working Paper Series*, http://wrap.warwick.ac.uk/108357/

Ramokapane M, Chowdhury PD, Domíngue A, et al.(2021). *Scope of Research Challenges for the Next Stage of Protecting Citizens Online Research Programme (REPHRAIN) V.1.1*. https://cpb-eu-w2.wpmucdn.com/blogs.bristol.ac.uk/dist/1/670/files/2021/05/REPHRAIN-Scoping-document-community-consultation-20.04.21.pdf access date 3rd June 2021.

Ruddick G (2016). *Admiral to Price Car Insurance Based on Facebook Posts*. The Guardian. 2nd November 00.01 GMT [Online]. Available at: https://www.theguardian.com/technology/2016/nov/02/admiral-to-price-car-insurance-based-on-facebook-posts (accessed on 27 April 2021).

Shapiro C and Varian HR (1997). *US Government Information Policy*. Berkeley: University of California. Unpublished manuscript https://www.researchgate.net/publication/248244291.

Shapiro C and Varian HR (1998). *Information Rules: A Strategic Guide to the Network Economy*. Boston, MA: Harvard Business Press.

Swire PP and Litan RE (1998). *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*. Washington, DC: Brookings Institution Press.

TECHNGI and The Willis Research Network (WRN) (2019). *AI & Next Gen Insurance Services Conference, Conference Thematic Summary and Overview*. https://www.techngi.uk/downloads/techngi-project-conference-thematic-summary-and-overview/.

Van Zandt T (2004). Information overload in a network of targeted communication. *RAND Journal of Economics*, 542–560.

Verborgh R (2017). Paradigm shifts for the decentralized Web. available at: https://ruben.verborgh.org/blog/2017/12/20/paradigm-shifts-for-the-decentralized-web/.

Zuboff S (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.

Author Biographies

Tzameret H. Rubin is a Senior Lecturer in Innovation and Management at Oxford Brookes Business School, Oxford Brookes University, UK. She holds a PhD in Economics from Macquarie Business School, Macquarie University, Sydney NSW Australia.

Tor Helge Aas serves as a professor of management at University of Agder, Norway. He holds a PhD in Strategy and Management from Norwegian School of Economics (NHH)

Jackie Williams is an impact coordinator and a research assistant at the School of Business and Economics at Loughborough University, UK.