Cambridge Law Journal, **81(1)**, March 2022, pp. 165–194
doi:10.1017/S0008197322000010

USE OF BIG DATA ANALYTICS AND SENSOR TECHNOLOGY IN CONSUMER INSURANCE CONTEXT: LEGAL AND PRACTICAL CHALLENGES

BARIŞ SOYER*

ABSTRACT. *Insurers are increasingly using big data analytics and artificial intelligence in rating risks and customising insurance products particularly in the context of consumer insurance. The primary aim of this article is to elaborate the extent to which the legal rules in force could ensure that consumers are not treated unfairly as a result of the use of such disruptive technologies. Relevant insurance law principles and doctrines are also considered as part of this analysis. The article concludes that despite the protection provided to consumers by data and consumer protection legislation, unregulated and unlimited use of data analytics and algorithms in the risk assessment process could create significant difficulties for consumers. It is argued that further regulation, especially making regular audits essential for insurers employing such technologies in risk assessment process, is required. The article also finds that the use of artificial intelligence in customising insurance products does not present similar degree of difficulties for consumers.*

KEYWORDS: *big data analytics, sensor technology, insurance law, legal issues emerging.*

I. INTRODUCTION

"Big data" in the consumer insurance context refers to the enormous data sets at the disposal of insurance providers which enable them to engage in cost effective, innovative forms of information processing for enhanced insight and decision-making.[1] This is normally made possible by algorithms capable of identifying patterns in the vast amount of data sets available. Once a pattern reliably emerges from the examination of data sets, it

* Professor of Commercial and Maritime Law at Swansea University. Address for Correspondence: Swansea University, School of Law, Singleton Park, Swansea, SA2 8PP, UK. Email b.soyer@swansea.ac.uk.

[1] As indicated by D. Boyd and K. Crawford, "Critical Questions for Big Data: Provocations for a Cultural, Technological and Scholarly Phenomenon" (2012) 15 Information Communication and Society 662, 663, "big data is less about data that is big than it is about a capacity to search, aggregate and cross-reference large data sets".

can be used as the basis for the operation of predictive analytics.[2] Machine learning plays a vital role in predictive analytics. It is one of the main ways in which artificial intelligence is being applied, with algorithms that can learn from examples and can improve their performance with more data over time.[3] Out of several machine learning models that exist, neural networks[4] and Bayesian networks,[5] are the ones often employed by insurers as part of risk assessment process.[6] Having learned from the new data and refined correlations, the algorithms are then able to fine tune their predictive power as well as making automated decisions. This is known as "deep machine learning", which is a branch of machine learning relying on complex statistical models and algorithms with multiple layers of parallel processing that loosely model the way the biological brain works and is used by insurers when analysing vast amount of data they gather on potential cover holders.

In addition to big data analytics, insurers today use various sensor technologies to obtain regular and real-time data from insurance subjects, which is often used not only as part of risk assessment exercise but also as the basis of offering individualised insurance products for their customers. For example, a telematics device, which is often plugged into the on-board diagnostic port of a vehicle,[7] collects information on driving behaviour, including geographical position, speed, acceleration and braking severity, vibration and impact events, and forwards it to motor insurers. Some home and contents insurers provide their customers the opportunity (and often incentives in the shape of discounts) to use home telematics devices, which are often connected to smoke alarms, carbon monoxide detectors, smart locks and doors and windows, and transmitted to inform insurers or customers instantly in case of an irregularity. Similarly, some life and health insurers provide wearables to their customers that gather and transmit real-time data about blood pressure, blood sugar and heart rate to insurers.[8]

[2] Predictive analytics is a branch of analytics concerned with making predictions as to the risk and probabilities of future events. Insurers have been using the basic principles of predictive analytics for decades, but today it is mainly used to produce reliable reports, which accurately identify levels of risk and aid in underwriting and policymaking by using a wide variety of methods, including data mining, predictive modelling, statistics, machine learning and artificial intelligence.

[3] See PwC, "Explainable AI: Driving Business Value through Greater Understanding", available at https://www.pwc.co.uk/audit-assurance/assets/explainable-ai.pdf (last accessed 15 August 2021).

[4] The idea behind artificial neural networks is to stimulate aspects of the behaviour of neurons in the human brain using the so-called perceptron algorithm. For a more technical explanation of how such networks operate, see S.J. Kwon (ed.), *Artificial Neural Networks* (New York 2011).

[5] Bayesian networks are often used for decision-making. For a more comprehensive and technical explanation of how such networks operate, see A. Darwiche, *Modelling and Design with Bayesian Networks* (Cambridge 2009). For a non-technical explanation of how different machine learning algorithms work, see S. Haddadin and D. Knobbe, "Robotics and Artificial Intelligence" in M. Ebers and S. Navas (eds.), *Algorithms and Law* (Cambridge 2020), 21–24.

[6] For the basic theory behind such models, see F. Rosenballt, "The Percepton: A Probabilistic Model for Information Storage and Organisation in the Brain" (1958) 65 Psychological Review 386.

[7] The same outcome can be achieved by installing an on-board diagnostic device (commonly known as a "black box") that is equipped with a SIM card to transmit data over the mobile network.

[8] Wearable personal technology is sometimes referred to as "fit tech".

Such wearables can also be used to monitor various aspects of an individual's well-being, including diet, weight, sleep and exercise.

It is envisaged that these new technologies have the potential to transform the insurance industry and customer experience particularly in two ways:

(1) The growing amount of data, increasing computing power and big data analytics allow insurance companies to identify risks in a much more granular and sophisticated manner (also known as "risk individualisation"); and
(2) The use of sensor technology enable the gathering of real-time and personalised data, allowing insurance companies to customise insurance products (also known as "risk customisation").[9]

It is anticipated that application of these new technologies could pose significant practical and legal hazards for consumers.[10] Broadly speaking, the primary objective of this article is to evaluate whether the current regulatory environment is fit to provide the desired protection for consumers.

There is no doubt that regulating artificial intelligence has been on the agenda of regulators for the last decade. Recently, for example, the European Commission has published a formal proposal for an EU Regulation to establish a uniform regulatory framework to deal with artificial intelligence systems.[11] Under these proposals, certain artificial intelligence practices (such as systems that have a significant potential to manipulate persons through subliminal techniques beyond their consciousness) are prohibited[12] and artificial intelligence systems that are deemed to be high-risk are only permitted subject to compliance with certain mandatory requirements and an *ex-ante* conformity assessment.[13] Obviously, the

[9] It is also possible that algorithms and artificial intelligence employed to manage claims and detect fraudulent patterns might function not in the manner programmed creating doubts on legitimate claims and leading ultimately rejection of such claims by insurers. This could lead to delays in the settlement process but one assumes that such mishaps can be addressed by insurers especially if affected individuals challenge the decisions reached with the aid of algorithms and raise complaints to authorities of the claim settlement processed employed.

[10] Some of these issues have been considered in other jurisdictions (e.g. T.E. Spahn, "Is Your Artificial Intelligence Guilty of the Unauthorised Practice of Law?" (2018) 24 Richmond Journal of Law and Technology 1; F. Thouvenin et al., "Big Data in the Insurance Industry: Leeway and Limits for Individualising Insurance Contracts" (2019) Journal of Intellectual Property, Information Technology and E-Commerce Law 209 and R. Swedloff, "The New Regulatory Imperative for Insurance" (2020) Boston College Law Review 2033) but as of today no comprehensive academic analysis has been carried out on the potential impact of big data from the perspective of law applicable in England and Wales.

[11] Commission Proposal 2021/0116(COD). The proposal defines artificial intelligence systems widely (Title I, art. 3) but there is no doubt that use of big data and machine learning for underwriting or risk customisation purposes will come under its scope.

[12] Title II, Article 5 of Commission Proposal 2021/0116(COD).

[13] Title III, Articles 6 and 7 of Commission Proposal 2021/0116(COD). Annex III, lists a limited number of high-risk AI systems, such as artificial intelligence systems used for biometric identification and categorisation of natural persons; systems intended to be used for recruitment or selection of natural persons for employment; systems intended to be used by public authorities to evaluate the eligibility

proposed regulatory framework will not apply in the UK[14] and currently the UK does not have a specific regulatory approach to artificial intelligence. However, the author is firmly of the view that developing an overarching regulatory regime could be rather problematic given that artificial intelligence systems are often employed for various purposes and normative values that need to be protected might differ significantly from one application to another. For example, using big data and algorithms might potentially have significant adverse impact on privacy of individuals and could have discriminatory consequences. On the other hand, using artificial intelligence in law enforcement might infringe on human dignity and impose significant restrictions on liberty. Hence, an overarching regime might fail to achieve the desired result.[15] One should also not lose sight of the fact that even if a framework akin to the proposed EU Regulation were to be put in place, it is highly unlikely that the use of big data and machine learning in risk rating process for underwriting purposes will be treated as a high-risk artificial intelligence system, and so it will be subject to less onerous regulatory requirements.

The thrust of this article is, therefore, to deliberate which fundamental values of consumers are at risk as a result of using big data and machine learning in risk individualisation and customising process. The author advocates that this area needs to be prioritised by regulators given the fact that using such systems on risk individualisation process could have adverse consequences on several fundamental rights of consumers and the fact that the current data protection and consumer laws fail to provide adequate degree of protection. To this end, the article sets out the scope and nature of such regulatory interference required specifically for the insurance sector to protect consumers from the unregulated and unlimited use of big data analytics by insurers.[16] On the issue of risk customisation (e.g. use of telematics), it is concluded that the current legal rules provide an adequate degree of protection for consumers unless, of

of natural persons for public assistance benefits and services and systems intended to be used by law enforcement authorities as polygraphs and similar tools to detect the emotional state of a natural person.

[14] That said, if the proposed EU Regulation finds its way into the statute book, it will certainly have implications for developers of such technologies within the UK trying to sell such systems to clients based in the EU or where they intend to use the outputs of such systems in relation to clients based in the EU.

[15] In fact, it has been often emphasised by legal theorists that adopting a particular normative value is bound to influence the nature and type of regulation. See e.g. T. Caulfield and R. Brownsword, "Human Dignity: A Guide to Making in the Biotechnological Era" (2006) 7 Nature Review Genetics 72; K. Tranter, "The Law and Technology Enterprise: Uncovering the Template to Legal Scholarship on Technology" (2011) 3 Law, Innovation and Technology 31. Similar points also made by various contributors in R. Brownsword, E. Scotford and K. Yeung (eds.), *The Oxford Handbook of Law, Regulation and Technology* (Oxford 2017).

[16] It is apparent that the same degree of protection would not be required in the commercial insurance context. Moreover, in some insurance sectors, such as marine, transport and aviation, where businesses based in various jurisdictions are the purchasers of such insurance, big data analytics might go a long way to bridge the information asymmetry between the assured and insurers.

course, sensor data is used by insurers as part of risk assessment process.[17]

II. Risk Individualisation

Algorithms and machine learning could enable insurance providers to profile each individual and the risk they pose to a much more granular degree. As a result of more precise risk profiling, as opposed to reliance on traditional generalised linear models to assess and price risk,[18] greater segmentation of risk pools defined by various factors (such as age, gender, health, work and social activity, shopping preferences and even social media activity) becomes possible. As the theory goes, this gives insurance providers an opportunity to assign each individual to a risk pool that better matches his/her attributes. As a result of such focused risk individualisation, individuals will no longer pay the average premium payable by those with whom they share a few actuarially relevant characteristics. At least, this is the message that insurers are pleased to promote as one of the breakthroughs facilitated by big data;[19] and there is evidence that some insurance providers have started using computer algorithms to this effect, especially in consumer insurance.[20] Naturally, insurers see this development as mutually beneficial, given that traditionally a considerable amount of employee time is spent on data processing.[21]

On the face of it, limiting situations in which individuals are expected to pay for the risk created and damage caused by others is a very attractive proposition. However, the devil is in the detail. It is submitted that "risk individualisation" facilitated by big data analytics could create numerous

[17] As discussed below, text to notes 82 and 83, the use of sensor data captured by telematics at the stage when the insurance contract is renewed as part of risk assessment process might create similar difficulties for consumers and should, therefore, be considered as part of any regulatory interference in this field.

[18] For a very good analysis of such models, see Casualty Actuarial Society, "Generalised Linear Models for Insurance Ratings" (2020) CAS Monograph Series No. 5 Second Edition, available at https://www.casact.org/pubs/monographs/papers/05-Goldburd-Khare-Tevet.pdf (last accessed 15 August 2021).

[19] It needs to be stressed that computer scientists have raised concerns on the effectiveness of algorithms in risk granulation process. E.g. it has been observed on several occasions that algorithms may act in unforeseeable ways. See in particular, the examples provided by A.H. Beck et al., "Systematic Analysis of Breast Cancer Morphology Uncovers Stromal Features Associated with Survival" (2011) 108 Science Transnational Medicine 1. It has also been noted that artificial neural networks, often used in insurance risk assessment process, show a high degree of opacity. This is because in such network, all learned information is not stored at a single point but is distributed all over the neural net by modifying the architecture of the network and the strength of individual connections between neurons (represented as input "weights" in artificial networks). See B. Walt and R. Vogl, "Explainable Artificial Intelligence: The New Frontier in Legal Informatics" (2018) Jusletter IT 22.

[20] See Financial Conduct Authority, Feedback Statement on Big Data Call for Inputs (2016) FS16/5, at [2.21], available at https://www.fca.org.uk/publication/feedback/fs16-05.pdf (last accessed 18 November 2021).

[21] See McKinsey Global Institute, "What Is Now and Next in Analytics, AI and Automation?", 8–9, available at https://www.mckinsey.com/~/media/mckinsey/featured%20insights/digital%20disruption/whats%20now%20and%20next%20in%20analytics%20automation/final%20pdf/mgi-briefing-note-automation-final.pdf (last accessed 15 August 2021).

difficulties that require further examination. In particular, unlimited and unregulated use of such analytics could infringe privacy of consumers as well as potentially having discriminatory consequences for those seeking insurance cover. Furthermore, as a result of a granular and more sophisticated risk assessment process some individuals might end up not being able to obtain insurance at all or can have access to insurance at a very high rate due to factors beyond their control, such as genetic predispositions. It is also possible that errors in the design of algorithms might create unintended consequences for consumers. The rest of this part will engage in a legal, technical and economic exercise with the objective of suggesting solutions to the problems emerging.

A. Privacy Issues

Given the enormous capability of software platforms, which apply risk prediction models based on algorithms, to derive and analyse data from various sources including internet searches, social media accounts, shopping and purchasing information obtained from credit card companies, it will not be an exaggeration to suggest that privacy of customers is in peril. It is very likely that consumers applying for motor insurance would not know what information is held about them and how that information is sought to be relied upon in assessing the risk. This information might potentially be harvested without informed consent and often without knowledge of the content generators.[22] There is also the risk that the information relied on for risk assessment may be inaccurate, though no opportunity is offered to the proposer to correct it. Such an intrusion of privacy could have adverse consequences for the consumer; and concerned about the consequences of their social network activities on their insurance premiums, some consumers might remove their social media accounts altogether.

However, perhaps the most alarming issue is the lack of any time restriction on the use of data obtained from a social media account or another source about an individual in terms of risk assessment. Against the legal background that a caution or even a conviction becomes spent after a certain period of time and does not need to be declared for most purposes,[23] it

[22] K. Crawford and J. Schultz, "Big Data and Due Process: Towards a Framework to Redress Predictive Privacy Harms" (2014) 55 B.C.L. Rev. 94, 94.

[23] Rehabilitation of Offenders Act 1974, s. 4, stipulates:

> "where a question seeking information with respect to a person's previous convictions, offences, conduct or circumstances is put to him or to any other person otherwise than in proceedings before a judicial authority –
>
> (a) the question shall be treated as not relating to spent convictions or to any circumstances ancillary to spent convictions, and the answer thereto may be framed accordingly; and
> (b) the person questioned shall not be subjected to any liability or otherwise prejudiced in law by reason of any failure to acknowledge or disclose a spent conviction or any circumstances ancillary to a spent conviction in his answer to the question."

might come as a surprise to most that in the new brave world of insurance algorithms, a moment of idiocy captured on a smartphone or posted on a social media platform creates a digital record and in principle remains accessible by insurers and others forever. Such data could be used by insurers to draw conclusions as to the lifestyle or personality of an assured applying for insurance.

1. Deploying the doctrine of good faith to ease privacy concerns

Privacy concerns in this context have led some commentators to seek refuge in a cornerstone doctrine of insurance law – utmost good faith – in order to provide a protection to consumers. It has been argued that the duty of good faith disclosure should be expanded to require insurers relying on big data to explain all risk-related information, to have an actuarial basis for the use of that information and to identify which risk factors have a particular bearing on the price of a particular risk.[24] Of course, this potentially gives the assured the opportunity to correct inaccurate data. The judicial justification given for this stance is section 17 of the Marine Insurance Act (MIA) 1906, which now simply stipulates that a contract of insurance "is a contract based upon the utmost good faith" without specifying any remedy.[25] It has been argued that this section by analogy could be used as the basis of implying a duty of disclosure to insurers to inform assureds of what information they hold following a risk assessment carried out by processing big data.[26]

Conceptually at least, such an expansion of the duty of good faith is plausible. The Consumer Insurance Disclosure and Representations Act (CIDRA) 2012, which applies to any individual "who enters into contract wholly or mainly for purposes unrelated to the individual's trade, business or profession",[27] does away with the insured's duty of disclosure.[28] However, the legislation is silent with regard to the pre-contractual position of the insurers. This presumably means that the general doctrine of good faith that applies to insurance contracts, as encapsulated in section 17 of the MIA 1906, in appropriate circumstances might enable courts to expand the application of good faith duty to require insurers to share the details of data they have acquired about the assured by using the power of big data. At this juncture, it should be mentioned that the Law Commissions did not envisage that the good faith doctrine would have such a role. In their view,

[24] B. McGurk, *Data Profiling and Insurance Law* (Oxford 2019), 158–64.
[25] Amended by Insurance Act 2015, s. 14(3).
[26] See McGurk, *Data Profiling and Insurance Law*, 221–25.
[27] CIDRA 2012, s. 1(1)(a).
[28] Accordingly, the main pre-contractual duty of good faith of the assured is to exercise reasonable care not to make a misrepresentation. In determining whether the consumer has exercised reasonable care depends on several factors such as (1) the type of policy taken out; (2) documentation presented to the consumer; (3) the nature of questions a consumer was asked; and (4) whether an agent was involved in procuring the policy.

the doctrine should continue as an interpretative principle but should not in itself give either party a cause of action.[29] However, as highlighted by several commentators already, this takes a rather narrow view of the doctrine[30] and is certainly out of line with the manner in which the good faith doctrine is developing in other jurisdictions.[31] Given that in the context of insurance contracts the parties are expected by virtue of the good faith doctrine to cooperate, it can hardly be suggested that it is unreasonable to expect an insurer at the pre-contractual stage to disclose data obtained from various sources about aspects of the risk or attributes of the assured.

Be that as it may, modelling the insurer's duty of disclosure in the context of consumer insurance contracts on the duty that exists in the context of business insurance contracts might not deliver the desired outcome. This is due to the nature of the materiality test that is relevant here. In a complex case concerning the extent of the insurer's duty of disclosure at the pre-contractual stage, the Court of Appeal in *Banque Financière de la Cité v Western Insurance Co Ltd.*[32] indicated that the insurer is expected to disclose all facts known to the insurer as long as such facts relate to "the nature of the risk sought to be covered or the recoverability of a claim under the policy which a prudent insured would take into account in deciding whether or not to place the risk for which he seeks cover with that insurer".[33] Adopting this test of materiality in the context of big data would mean that insurers are expected to disclose those facts which have been actuarially shown to be objectively relevant to the level of the risk. Accordingly, insurers who profile risks by reference to non-causal risk proxies (such as social media posts or shopping habits) will not necessarily be required to disclose them even if it is assumed that they need to operate under the umbrella of pre-contractual duty of good faith.

Therefore, the nature of the "materiality" test in this context imposes a significant limitation on the prospect of the good faith doctrine providing

[29] Law Commission and Scottish Law Commission, *Insurance Contract Law: Business Disclosure: Warranties, Insurer's Remedies for Fraudulent Claims; and Late Payment*, Cm. 8898, SG/2014/13, Ch 30.8.

[30] B. Soyer and A.M. Tettenborn, "Mapping (Utmost) Good Faith in Insurance Law – Future Conditional?" (2016) 132 L.Q.R. 619, 622–29, 634–35. Some commentators, on the other hand, have taken a more conservative view of the role that good faith doctrine could play in post contractual context, see e.g. M.C. Hemsworth, "The Fate of 'Good Faith' in Insurance Contracts" [2018] L.M.C.L.Q. 143.

[31] R. Merkin and Ö. Gűrses, "The Insurance Act 2015: Rebalancing the Interests of the Insurer and the Assured" (2015) 78 M.L.R. 1004, 1026–27. See also Soyer and Tettenborn, "Mapping (Utmost) Good Faith", 631–32.

[32] *Banque Financière de la Cité v Western Insurance Co. Ltd.* [1990] 1 Q.B. 665, reversing the judgment of the first instance [1987] Lloyd's Rep. 69.

[33] Ibid., at 772. This approach to materiality found considerable support at the House of Lords, when an appeal to the Court of Appeal judgment was advanced, even though it was not necessary to apply it to solve the case. Lord Templeman described the reasons given by the Court of Appeal as "cogent". Lord Jauncey put it in these terms [1991] 2 A.C. 249, 281: "Thus any facts which would increase the risk should be disclosed by the insured and any facts known to the insurer but not to the insured, which would reduce the risk, should be disclosed by the insurer."

protection for consumers. The author also has significant doubts whether the good faith doctrine is the appropriate way forward in this debate, and these concerns will be elaborated further next.

First, these algorithms are by nature very complex, making it difficult even for programmers to unravel and explain how they have reached a particular underwriting decision. In fact, computer scientists warn that in most systems it is not usually possible to interpret and explain the role of the different variables.[34] That being the case, one might forcefully query how realistic it is to expect insurers to be able to explain to every assured the weight of the personal data used in the decision-making process.

Second, it should be noted that such an expansion of the good faith doctrine might be at odds with its *raison d'être*. Traditionally, one of the main justifications for the good faith doctrine is to deal with information asymmetry.[35] Accordingly, the primary function of the good faith doctrine is to ensure that the party to a contract who has the command of information about the risk does not abuse the other party who has no information about various risk factors. Given that it is the consumer who is the generator of the personal data in question, it is difficult to see how an insurer who attempts to make sense of such unstructured data with the purpose of being able to make an underwriting decision is in a better position (knowledge-wise) than the assured so that it needs to disclose to the assured details of the risk assessment process assisted by big data analytics to achieve information equilibrium.

Third, before advocating an expansion of the insurer's duty of good faith at the pre-contractual stage, it is worth bearing in mind the evaluation of the doctrine of good faith in consumer insurance, and other developments. Less than a decade ago, it was deemed appropriate to remove the duty of disclosure at the pre-contractual stage for consumers with the introduction of CIDRA 2012. The justification given for this was that insurers now have at their disposal various advanced data collection tools so that they can obtain the data that they need to be able to engage in a rational risk assessment exercise. So, in fact it was the policy-makers who instructed insurers to use big data and other tools (i.e. machine learning, algorithms) and not expect any disclosure about the risk from consumers, as the latter might not appreciate what they need to disclose. Since then, a new data protection legislation has been put in place to ensure that data processors, including insurers, act in a reasonable fashion when dealing with personal data.[36] So, does it make sense to expect the insurers to disclose to consumers the fine details of the process of risk rating their algorithms undertake,

[34] See The Geneva Association, "Promoting Responsible Artificial Intelligence in Insurance", 11, available at https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/ai_in_insurance_web_0.pdf (last accessed 15 August 2021).

[35] *Greenhill v Federal Insurance Co. Ltd.* [1927] 1 K.B. 65, 76 (Scrutton, L.J.).

[36] Effectiveness of the relevant data protection legislation will be deliberated in the succeeding part.

especially given that in most cases it will not be possible to explain this? If we do expect such disclosure, there is a serious risk that this might result in a waste of effort and money in placing insurance that might push the cost of insurance up, potentially wiping out the benefits of having a more granular risk assessment for individuals.

2. Protecting privacy with the aid of data protection legislation?

On the premise that the long-established insurance law principle of good faith would not be an appropriate tool to ease the privacy concerns of consumers, the next logical step is to consider whether data protection legislation could provide the appropriate level of protection for consumers whose personal data has been harvested and used by insurers for risk assessment purposes. The relevant legal framework in this context can be found in UK General Data Protection Regulation (UK GDPR), which is based on EU General Data Protection Regulation,[37] and the Data Protection Act 2018, designed to supplement UK GDPR. There is no doubt that these legislative measures impose several limitations on the manner in which insurers could use big data analytics and other forms of artificial intelligence for risk assessment purposes.

As a starting point, we should emphasise that these pieces of legislation do not prohibit insurers from obtaining personal data[38] relating to consumers seeking insurance cover directly or from third parties for the purpose of processing (for risk assessment purposes) as long as various safeguards are observed.[39] In particular, under this legislation insurers, as data controllers, engaged in processing special categories of data[40] would require explicit consent from their customers.[41] This would naturally require a high degree of precision and definiteness in the declaration of consent, as well as a precise description of the purposes of processing. Of course, this is

[37] Regulation (EU) No 2016/679 (OJ 2016 L 119 p.1). The UK GDPR is established by the European Union (Withdrawal) Act 2018, which incorporates the body of EU law (including the GDPR) as it exists on the day of Brexit, into UK law thereafter.

[38] UK GDPR, Article 4(1), defines "personal data" as "any information relating to an identified and identifiable natural person".

[39] Most significantly, it is essential to determine from the outset the purposes of processing data. The processing of personal data for undefined or unlimited purposes is unlawful as it does not enable the scope of the processing to be precisely delimited (art. 5 of UK GDPR). Article 15 of UK GDPR gives the data subjects (here consumers) right to request from data controllers (insurers) more extensive information about the personal data processed about them including the legal basis of processing, the period of data storage, information about access and other rights over the data (including the right to complain to the Information Commissioner Office). Last but not least, insurers engaged in data processing for risk assessment purposes would be required to engage in piracy impact assessment (art. 35 of UK GDPR).

[40] Personal data in this context refers to data revealing "racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; the processing of genetic data for the purpose of uniquely identifying an individual; the processing of biometric data for the purpose of uniquely identifying an individual; (d) the processing of data concerning health; the processing of data concerning an individual's sex life or sexual orientation" (art. 9(1) of UK GDPR).

[41] Article 9(2) of UK GDPR.

a significant safeguard but in practice insurers, with the assistance of their lawyers, employ a clear wording in their privacy notices to achieve this consent from those seeking insurance cover and it is always a debatable point whether consumers giving consent really appreciate to what they are consenting.[42]

Another safeguard that can, potentially, provide a degree of protection for consumers is the provision of UK GDPR that gives data subjects a right not to be subjected to a decision based solely on automated processing (in this context "profiling") of personal data.[43] Again, the protection that this can provide to consumers should not be overstated. The insurers will, in all probability, obtain consent to carry out automated decision-making,[44] and in that case the only right of the consumer will be to seek *ex post* an explanation of automated decisions affecting them.[45] In the unlikely event that such content is not expressly obtained, it is also possible for insurers to argue successfully that profiling activities for underwriting purposes should be permissible as they are necessary for entering into, or performance of, a contract between themselves and the data subject.[46] However, this clearly does not require insurers to disclose the "full algorithm" and they can easily standardise the information provided with the aid of their lawyers to satisfy this requirement.

3. Suggested solution for privacy concerns

As discussed above, the data protection legislation provide certain safeguards, which can ease some of the privacy concerns of consumers, but it is submitted that there are still gaps left by the regulatory law that can compromise the privacy of individuals:

[42] For more detailed discussion on this point, see R. Brownsword, *Rights, Regulation and the Technological Revolution* (Oxford 2008), ch. 3.

[43] Article 22.

[44] It is very common today for insurance companies to require customers to sign consent forms giving them authority to undertake automated decision-making with regard to pricing and underwriting. See e.g. the consent form used by one insurer: Insurance Corporation, "Customer Privacy Notice & Consent Form", available at https://www.insurancecorporation.com/wp-content/uploads/2018/05/ICCI-Customer-Privacy-Notice-and-Consent-Form.pdf (last accessed 15 August 2021).

[45] Articles 13 and 14 of the UK GDPR. For a detailed analysis on this matter, see M. Brkan, "Do Algorithms Rule the World? Algorithmic Decision Making and Data Protection in the Framework of the GDPR and Beyond" (2019) 27 International Journal of Law and Information Technology 91.

[46] Article 22(2)(a) of UK GDPR. It should be noted that there is no clarification as to how this criterion will apply in practice in the relevant legislation so it is ultimately left to the courts to determine but it is unlikely that the criterion of being "necessary" connotes indispensability. As indicated by I. Mendoza and L. Bygrave, "The Right Not to Be Subjected to Automated Decisions Based on Profiling" in T.-E. Synodinou et al. (eds.), *EU Internet Law: Regulation and Enforcement* (New York 2017), 92, it is hard to find an example where an automated decision without human involvement has to occur. The same authors also suggested that, at 92, this criterion is presumably added to the GDPR to make it difficult for controllers to remove the right of subject matter to deny being subjected to such automated decision-making (art. 22(1)) simply by pointing to standardised contract with the subject matter. For more detailed examination on this issue, see D. Sancho, "Automated Decision Making under Article 22 GDPR: Towards a More Substantial Regime for Solely Automated Decision-making" in Ebers and Navas, *Algorithms and Law*, 136.

(1) A time limit should be imposed as to how far back insurers can go in gathering and using personal information concerning individuals. To give an extreme example, it will not be appropriate to allow algorithms to use, as part of the risk assessment exercise, comments placed on social media years ago by an individual. The data controller is expected to review the need for the continued storage of personal data[47] but no restriction is imposed on how far the data controller can go back in terms of collecting personal data.[48] This is an area that requires a careful re-evaluation.

(2) The principles of transparency and purpose limitation that underpin the UK GDPR require insurers to inform data subjects if the data originally collected for a different purpose (i.e. data obtained from credit card companies concerning shopping habits of individuals) is used for a different purpose (i.e. running big data analytics to calculate individual premiums for health insurance; this is known as data repurposing).[49] While privacy notices could be used to inform customers about such repurposing, it might be difficult, if not impossible, for insurance companies to comply with this requirement if their analysis includes data about individuals who are not their customers. As put by one commentator: "Insurance companies using data mining techniques do not usually know what they will find until it is too late."[50] Therefore, it certainly makes sense to consider imposing some specific restrictions on insurance companies' capacity to repurpose data.

(3) The increase in the volume and variety of data flows renders the data more susceptible to unwitting manipulation, use or disclosure; and of course there is an increased risk of the data being stolen or compromised as a result of a cyber-attack. The risk could be even higher if insurance companies delegate the task of running analytics to smaller "insurtech" providers, given that security systems of such companies might be easier to penetrate by external forces. It is, therefore, necessary to consider putting in place specific requirements as to how personal data should be protected by insurance companies; and no doubt procedures must be put in place with core security standards, prompt notification and remediation of breaches. The data protection legislation require data controllers to put in place technical and

[47] Article 5(1)(e) of UK GDPR.

[48] There is, of course, a general principle in UK GDPR, Art 5(1)(a), which requires any data processing to be conducted fairly and it is possible that an individual could challenge an insurer's decision to utilise personal data going back a long time on that ground. However, the fairness requirement under the Act is very subjective and there are no clear guidelines (or case law) as to how fairness in the process of processing personal data could be achieved. The key issue will be whether an insurer in this context could justify the use of such data for the purpose of a balanced risk assessment of the risk proposed.

[49] Article 5(1)(b) and (c) of UK GDPR.

[50] P. MacDonnell, "The European Union's Proposed Equality and Data Protection Rules: An Existential Problem for Insurers" (2015) 35 Economic Affairs 225, 233.

organisational measures to ensure no accidental loss of personal data occurs[51] but there is a case to consider standardising such procedures for insurance providers engaged in big data analytics due to the sheer and varied amount of information their algorithms use for risk assessment purposes and the significance of ensuring the integrity of such data from the perspective of consumers.

In essence, there is no doubt that relevant data protection legislation affords a degree of control to individuals over their personal data, and requires insurers to ensure certain safeguards are in place to be able to process such data with the aid of artificially intelligence enabled processes. However, two preliminary observations are in order. First, it is not clear that individuals consenting to such data processing are fully aware of how much personal data concerning themselves can be obtained by insurers and how that data can be used as part of processing. In that sense, it is debatable whether their consent is actually an informed one. More fundamentally, given the significant consequences such risk assessment might have on the legal position of an individual, it can plausibly be argued that those who are left in the mercy of algorithms deserve more protection than that provided to them by the data protection legislation.

So, what is the way forward to protect the privacy of consumers in the big data era? It is proposed that guidelines should be developed and imposed by regulators, possibly by the Financial Conduct Authority (FCA),[52] as to the ethical use of big data for risk assessment purposes. Such regulations could restrict the use of data along the lines discussed above: namely, imposing limitations with regard to how far back in time personal data could be searched; restricting repurposing of personal data for insurance purposes, and stating the nature of specific safeguards that must be put in place by insurers engaged in big data analytics. These considerations should also comprise the steps that need to be taken to protect such data against cyber risks. Such regulations could be included in the FCA Handbook, in the sourcebooks of particular relevance to the conduct of insurance business.[53] The collaboration of the insurance sector, and organisations such as Association of British Insurers (ABI), at early stages of the development of such guidelines would be beneficial, especially given that this is an emerging area where expertise and previous experience are limited. In order to encourage insurers to remove any barrier to accountability, it is also recommended that a new agency, that will undertake random

[51] See Article 25(2) of UK GDPR.

[52] As the body tasked in ensuring the honest and fair functioning of insurance market and protection of consumers.

[53] The Conduct of Business Source Book (COBS) and Insurance: Conduct of Business Sourcebook (ICOBS). The former applies to firms that carry our life insurance business, and the latter to firms that carry out insurance business.

auditing of the algorithms used by insurers to ensure that various algorithms in use function within the approved bounds, is established by regulation. This new agency should have expertise to deal with technical issues relating to algorithms, but it is also essential that those serving in that unit have a good understanding of insurance law and regulatory guidelines developed by the FCA. It is submitted that an agency of this nature would serve the function of policing the use and development of algorithms to ensure that they comply with the standards on human rights. No doubt, further deliberation is necessary as to the precise powers of this agency, its relationship with other regulatory bodies and how it will be funded. These are significant matters that need to be considered with the involvement of insurance and consumer representatives and regulators.

B. Discrimination

Obviously anti-discrimination legislation would not allow the use of data that have a high risk of discrimination through having a considerable disparate impact on protected characteristics. In the UK, the Equality Act 2010 is the basis for this kind of legal protection; it prevents insurers from using algorithms that would seek information that might lead to a discrimination based on protected characteristics (i.e. age, disability, gender assignment, marriage or civil partnership, race, religion or belief, sex and sexual orientation).[54]

This much is clear and uncontentious. It is possible that indirect discrimination could still take place even though the algorithms used are not programmed to take into account a protected characteristic in risk individualisation process but the actual effects of individualisation carried out by the algorithms would be particularly disadvantageous for people possessing a protected characteristic.[55] Several commentators share the view that this kind of discrimination (also known as "unintentional proxy discrimination") is the inevitable consequence of algorithms which are designed to find linkages between input data and target invariables, irrespective of the nature of these linkages.[56] For example, a programme would obviously not be designed to discriminate against women, but certain proxies, such as the colour or model of the car, might accidentally recreate side effects or bias that a human would not have voluntarily incorporated into the system. It is also possible that unintended discrimination could creep in as a result

[54] Equality Act 2010, ss. 4–12.

[55] It is worth noting that this is recognised as "indirect discrimination" under Equality Act 2010, s. 19, and is prohibited.

[56] J.M. Skopek, "Big Data Epistemology and Its Implications for Precision Medicine and Privacy" in I.G. Chen et al. (eds.), *Big Data Health and Bioethics* (Cambridge 2008), 30; S. Barocas and A.D. Selbst, "Big Data's Disparate Impact" (2016) 104 C.L.R. 671, 712; L. Edwards and M. Veale, "Slave to the Algorithm? Why A 'Right to Explanation' Is Probably Not the Remedy You Are Looking For?" (2017) 16 Duke L. Tech. Rev. 18, 25.

of the data used to train algorithms not being sufficiently representative. Put differently, biased training data may lead to discriminatory models either because the training data may view historical data influenced by prejudice as valid examples or it may draw inferences based on a limited or biased sample of the population.[57] One should also not dismiss the possibility that algorithmic learning can go awry resulting in unintended discrimination. Computer scientists have discovered that a neural network called CycleGAN, used in image to image translation, learned to hide information concerning the original image inside the generated one in the form of a low-amplitude high-frequency signal.[58] This was not an isolated case and it is obvious that a similar mishap could arise in the operation of algorithms used by insurers for risk assessment purposes potentially leading to unintentional proxy discrimination.

What options are open to regulators to eliminate unintended discrimination that can arise as a result of a high volume of data that can be obtained and analysed by algorithms? Regulators can employ various techniques to prevent this kind of discrimination happening. Perhaps the most straightforward solution to the problem of discrimination fuelled by big data is to allow only certain pre-approved variables, determined by regulators, to be used by algorithms in the risk assessment process. This might be easy to implement, but it will also remove most of the benefits that granular risk classification brings. Put differently, this kind of solution is counterproductive, as it will take away the innovative edge that big data analytics brings to insurance practice. Also, this solution does not tackle the problem of algorithms or data collection systems being adversely affected by human prejudice.

Another potential solution is to allow insurers to use any data legally available but require them to explain to regulators the impact of their algorithms on members of protected groups.[59] This might work if insurers are able to explain that a variable used in risk assessment and causally linked to the desired outcome (risk individualisation) is not acting as a proxy for a protected characteristic. Of course, showing a causal link in this context is not an easy task, but regulators could set the standard of proof low and expect a plausible causal link to be shown rather than requiring a definitive proof of causality.[60] The task is by no means a simple one, but it will certainly mean less interference from the regulators. The

[57] Barocas and Selbst, "Big Data's Disparate Impact", 680; see also The Geneva Association, "Promoting Responsible Artificial Intelligence", 12–13.

[58] C. Chu, A Zhmoginov and M Sandler, "CycleGAN, a Master of Steganography" (2017) NIPS Machine Deception Workshop arXiv:1712.02950.

[59] S. Hoffmann, "Big Data's New Discrimination Threats: Amending the Americans with Disabilities Act to Cover Discrimination Based on Data-driven Predictions of Future Disease" in G. Cohen, H.F. Lynch and E. Veyena (eds.), *Big Data, Health Law, and Biometrics* (Cambridge 2018), 85.

[60] J. Gaulding, "Note, Race, Sex and Genetic Discrimination in Insurance: What's Fair?" (1995) 80 Cornell L. Rev. 1646, 1681.

regulators[61] will have to audit insurers' classification systems randomly looking at the "data sets mined" by algorithms as well as the "source codes and programmers" notes' describing the variables, correlations and inferences embedded in the algorithm.[62] These audits should focus on whether personal data is appropriately scrubbed from the data used to create predictions, whether insurers are gathering inappropriate individual data (these dealing with privacy issues discussed in earlier part) and whether the data are suggesting inappropriate correlative predictions. As indicated earlier, it is vital that the personnel carrying out such audits have sufficient technical and legal knowledge to be able to assess the appropriateness of the algorithms used for risk individualisation.

C. Errors and System Vulnerability

As has already become clear from the discussion, algorithms used for data profiling operate on the basis of correlation, not causation. This creates a risk that the algorithms might at times find correlation in the data analysed with statistical significance even though there is no meaningful correlation between the variables.[63] An example suffices to illustrate the issue. A big data analysis might reveal that from 2006 to 2011, the US murder rate correlated well with the market share of Internet Explorer, as both went down sharply, but it is hard to imagine that there is any meaningful causal relationship between the two.[64] Also, it should be borne in mind that due to the large scale of data processed by such algorithms, a small systematic error might have far-reaching consequences in terms of risk assessment.

Whilst this is not something attributable to the way algorithms operate, it should also be kept in mind that input errors or missing data on the documents or data that have been analysed could also contribute to inaccurate risk profiling by algorithms. The health sector, in particular, is susceptible to such errors. For example, it has been observed in the US that clinicians entering data into electronic health records may choose erroneous diagnosis codes, check boxes incorrectly or uncheck boxes inappropriately if the default setting has all boxes checked.[65] Similarly, data about treatment outcomes is often missing from electronic health records. Patients who are given medications, such as antibiotics, are not often asked to return to the doctor and report on their progress. This might lead to a situation where the patient's health record will detail the diagnosis and prescription

[61] This task could alternatively be undertaken by the new agency suggested in Section II(A)(3).
[62] D.K. Citron and F. Pasquale, "The Scored Society: Due Process for Automated Predictions" (2014) 89 Wash. L. Rev. 1, 23.
[63] This is technically known as the "problem of overfitting".
[64] G. Marcus and E. Davies "Eight (No, Nine!) Problems with Big Data", *New York Times*, available at https://www.nytimes.com/2014/04/07/opinion/eight-no-nine-problems-with-big-data.html (last accessed 15 August 2021).
[65] F. Magrabi et al., "An Analysis of Computer-related Patient Safety Incidents to Inform the Development of A Classification" (2010) 17 J. Am. Med. Inform. Assoc. 663, 665, 669.

but will not indicate whether the patient has recovered or failed to improve and sought treatment from a different specialist.[66]

Last but not least, it is hardly an overstatement to suggest that cyber risks, whether unintentional (e.g. program bugs) or intentional (e.g. malicious cyber attacks), will become increasingly more significant as more insurers begin to employ artificial intelligence and rely on big data analytics for risk assessment. Any bug or infiltration of the programmes used for data analysis could lead to the system making extremely suboptimal decisions.

The author's intention by highlighting these difficulties is to stress the point that to use the potential of big data analytics in insurance law, there is a need to consider putting in place a regulatory framework requiring how such algorithms should operate, and to introduce an audit requirement carried out by regulators (or the new agency set up for this purpose) on the systems that will be employed by insurers.[67] That way any potential vulnerabilities and errors in the system or in the manner data is collected could be identified and eliminated.

D. Insurability Problem

One potential problem associated with an increased level of risk individualisation as a result of big data analytics is that insurance might become unaffordable or unavailable for certain groups of people. Imagine a consumer who has a genetic predisposition that raises the risk of a certain illness. This is clearly a factor beyond that individual's control; but big data analytics, armed with additional data such as medicines ordered by that individual from the internet, or searches undertaken by that individual with regard to certain medical conditions, might enable insurers to place that individual into a high-risk category, making life insurance or critical illness insurance cover unaffordable. This may raise social concerns, in particular if the risk is correlated with low income and low wealth. It is a relief that in the UK the potential destructive impact of indiscriminate use of genetic data on certain individuals has attracted attention. The ABI entered into a voluntary moratorium with the Government in 2011,[68] which commits insurers offering life, critical illness and income protection insurance not to ask their customers about predictive genetic test results when applying for insurance.[69]

[66] C. Newgard et al., "Electronic Versus Manual Data Processing: Evaluating the Use of Electronic Health Records in Out of Hospital Clinical Research" (2012) 19 Acad. Emergency Med. 217, 225.

[67] See the discussion above in Section II(A)(3).

[68] Association of British Insurers, "Code of Genetic Testing and Insurance", available at https://www.abi.org.uk/globalassets/files/publications/public/genetics/code-on-genetic-testing-and-insurance_embargoed.pdf (last accessed 15 August 2021).

[69] This voluntary agreement is still in force but it does not apply to diagnostic genetic tests, nor does it apply to non-genetic medical tests (i.e. blood or urine tests for cholesterol, liver function or diabetes).

This is a positive development,[70] but, given the immense potential big data analytics presents to individualise risks, it is necessary to give some thought as to whether there are other sectors in which risk individualisation should not be allowed. One example is risks created as a result of climate change. If big data analytics have the capability of identifying certain correlations making it difficult for consumers who live in a particular location to obtain insurance cover for their homes, policy-makers should consider whether the solidarity principle should prevail to prevent such data from being available for risk assessment purposes.[71]

Another area that requires attention is the position of those who will not be able to purchase insurance at an affordable rate as a result of granular risk profiling provided by algorithms. Assume the position of an individual who does not suffer from any genetic disorder but is not leading a healthy lifestyle and as a result of big data analytics (e.g. information obtained from his/her medical records, internet searches, shopping and eating habits), s/he is identified as a bad risk. Naturally, most insurance providers will refrain from offering him/her life or critical illness insurance at an affordable rate or at all. This might pose a problem for the government. On one hand, given that this individual's predicament is the result of his/her choices, one can plausibly argue that there is no need for government or industry interference. Equally, it can be argued that in the absence of such granular risk assessment this individual would have been offered insurance at a reasonable rate so s/he should not be penalised due to the fact that technology allows us to better profile risks. The author has less sympathy for the latter argument; however, if the government decides to intervene in this instance, the next issue is going to be deciding the nature of such intervention. One possibility is to provide premium subsidies to those who are in that category. Some commentators believe that providing premium subsidies is the best form of intervention to an insurance market, as this does not distort the price mechanism, leading to inefficiencies, and allows positive effects of premium differentiation to be maintained.[72] An alternative could be to establish a scheme of insurance of last resort for such individuals similar to Flood Re. However, it should be noted that the position of those who

[70] The position is similar in many other jurisdictions. E.g., in Switzerland, insurance companies are barred from utilising pre-symptomatic or prenatal genetic tests in their underwriting process (Federal Act on Human Genetic Testing (HGTA), art. 27).

[71] On a related matter, in the UK in areas where there is serious risk of flooding, insurers could pass part of their exposure to a reinsurance company established for this purpose, Flood Re. This arrangement has been put in place to ensure that insurers do not refrain from insuring house cover to individuals living in locations susceptible to flooding. The pool of money to cover claims made on policies which are in the scheme will come from two places – the charge for each policy which is passed into Flood Re, and an additional annual £180 million levy on UK home insurers. Flood Re also has its own reinsurance policy in place to ensure it will be able to cope with significant or multiple floods. This arrangement is a good illustration of intervention to the market in an area where risk individualisation would have reduced the prospect of finding adequate insurance cover.

[72] See C. Kousky and H. Kenreuther, "Addressing Affordability in the National Flood Insurance Programme" (2014) 1 Journal of Extreme Events 1450001.

price themselves out of the insurance market due to their personal choices is not similar to those who happen to own a house exposed to natural disasters created by external factors. It is therefore unlikely that government would be willing to invest into an insurance scheme to protect them. Still, as the use of data analytics becomes more common, this would bring these issues to the fore, and there is a need for them to be more thoroughly debated.

E. Price Discrimination

A controversial aspect of big data analytics is that it might potentially enable insurers to determine which of their customers are sensitive to prices so that they can charge higher prices to those willing to pay more. Essentially, this means that insurers could use non-causal risk proxies (e.g. shopping habits or internet searches) to determine whether a potential customer is willing to pay more for the same product as opposed to others who are in the same risk category. Put differently, the big data analytics might provide insurers with a very powerful weapon so that they quantify the premium the customer will be asked to pay based on their willingness to pay rather than their riskiness. Most insurers will view this as part of their price optimisation strategy, although this might not be a view widely shared by most consumers.[73] It is also worth noting that such practices are banned in some jurisdictions.[74]

The arguments on this matter are finely balanced but it is submitted that no interference from regulators is necessary for the following reasons:

(1) Judged purely from an economic perspective, it is possible that price discrimination might have a positive effect on society. Assuming that additional profits generated from those who are willing to pay more for their insurance cover are used by insurers to offer insurance to those who would normally not be willing to purchase insurance at the going rate, this will contribute to an expansion of insurance in the population. Insurers might see a benefit in engaging in this kind of exercise to maximise their profit margins by attracting new business, and they could use the additional funds generated from price discrimination as an incentive to this end.
(2) Approaching the issue from a behavioural economics perspective, it is possible that some consumers might benefit further from price discrimination. Imagine that a consumer is quoted a premium by an

[73] Empirical studies have shown that price discrimination will often be regarded as unfair if it exceeds a certain level. See e.g. K.L. Haws and W.O. Bearden, "Dynamic Pricing and Consumer Fairness Perceptions" (2006) 33 Journal of Consumer Research 304.

[74] In California, for example, the Insurance Commissioner has prohibited price optimisation in his Notice Regarding Unfair Discrimination in rating: Price Optimization. Price optimisation has been described as "any method of taking into account of an individual's class or willingness to pay higher premium relative to other individuals or classes".

insurer slightly lower than other offers. To an insightful consumer this is a signal that s/he is regarded by that insurer, following an assessment by data analytics, as a low-risk customer, enabling such customer to use this information against the insurer by insisting on an even lower premium. Taking this theory to its natural conclusion, one might suggest that in a world in which insurers know more about policyholders than the latter know about themselves, pooling and attendant risk-spreading will actually increase, and to be able to stick to the pool rate will be the best the insurers can hope to do.[75]

(3) In a market which functions in an efficient manner, there is every reason to believe that competition between insurers will restrict their ability to exert aggressive price discrimination.

(4) Last but not least, from a regulatory perspective it remains a possibility that a consumer could claim that an extreme degree of price discrimination based on non-causal risk proxies is a violation of the FCA Principles for Business (PRIN) Handbook[76] or the rules in ICOBS,[77] enabling him/her to make a complaint to Financial Ombudsman Service[78] or bring a claim for damages against a regulated insurance provider under s. 138D of the FSMA 2000.[79] Put differently, there are legal mechanisms open to any individual who can show that s/he has suffered from the effects of price discrimination.

III. Risk Customisation

Sensor technology, by increasing connectivity and enabling continuous monitoring through the mobile network, provides opportunities for insurers to use various technological devices to obtain real-time data on the subject matter of insurance. There is no denying that the use of such devices could yield several benefits for the assured. It is possible, for example, that such digital monitoring could provide real-time insights to policyholders on their risk behaviour and incentivise them to reduce their risk. Also, continuous collection and analysis of behavioural data enables dynamic risk

[75] P. Siegelman, "Information and Equilibrium in Insurance Markets with Big Data" (2014) 21 Conn. Ins. L.J. 317, 333–36.

[76] E.g. PRIN Handbook 2.1.1.1 reads: "A firm must conduct its business with integrity." In a similar vein, 2.1.1.6 requires that "a firm pay due regard to the interests of its customers and treat them fairly".

[77] ICOBS 2.5.1 reads: "A firm must act honestly, fairly and professionally in accordance with the best interests of its customer."

[78] Financial Services and Markets Act (FSMA) 2000, s. 228(2), provides that a "complaint is to be determined by reference to what, in the opinion of the ombudsman, is fair and reasonable in all circumstances of the case".

[79] This provision enables persons who suffer a loss as a result of a breach of a rule made by the FCA to have a right of action for those losses. The measure of damages under this provision is likely to be no different from that which could be recovered for breach of contract or tort and the same approach to causation, foreseeability and remoteness is likely to apply (see *Rubenstein v HSBC Bank Plc* [2011] EWHC 2304 (Q.B.), [2011] 2 C.L.C. 459, [117] (H.H.J. Havelock-Allan).

assessment, providing an opportunity for consumers to obtain personalised insurance cover. This would potentially mean a reduction in motor insurance premiums for better drivers and cheaper life/critical illness cover to those who eat healthy diets and exercise a lot. Consumers could also benefit from the additional variety of products that insurers can offer as a result of the use of such devices. In motor insurance, for example, several insurers offer use-based insurance by using telematics devices to help them to determine with precision how much the insured vehicle is used and in what geographical limits.

Approaching the matter from the perspective of insurance law, one can envisage such devices having a particular impact on two aspects of the insurance relationship:

(1) Insurers could use the additional real-time data obtained as part of the risk assessment process to determine the premium for renewals or extensions; and
(2) Insurers could add new clauses into the contract designed to limit and/or control the alteration of risk detected using the additional data.

There can be no doubt that using the real-time data obtained by sensor technology in risk assessment process could raise issues, such as privacy and discrimination, as discussed in the earlier part, as well as some other legal issues.[80] On the other hand, as will be deliberated further in this part using such real-time data as a means of limiting the scope of cover do not create similar problems for consumers.[81]

A. Impact of Sensor Data on Risk Assessment

The fact that such devices will provide insurers with real-time data on key matters concerning the risk (e.g. driving habits or lifestyle of the assured) means that insurers will have at their disposal significant amount of additional data for risk assessment purposes. In recent years we have witnessed insurers using this additional data creatively. Some insurers, for example, offer the assured the prospect of reducing the insurance premium if it is established with the aid of this additional data that the risk score of the assured is better than the score calculated at the outset. However, it is certain that the additional real-time data will be of great assistance to insurers when they consider offering renewals or extensions to the cover. At this juncture, a difficulty highlighted earlier might reoccur. It is a serious possibility that a consumer might find it difficult to obtain insurance cover at an affordable premium if the data transmitted through such devices contribute to him/her being classified as a bad risk. If this is the consequence of an

[80] See text to notes 82–88 below.
[81] See text to notes 90–112 below.

individual's behaviour, the author has less sympathy. However, the matter is slightly different when it comes to health or life insurance. The real-time data obtained from individuals with high health-related risks (not induced by their own lifestyle choices) would mean that they will face high and potentially unaffordable premiums which would no doubt limit their access to basic medical service provision, leading to a further deterioration of their condition. As discussed above, this is an area that requires further discussion, especially as to whether a regulatory interference to the market conditions would be required.[82] By the same token, using real-time data obtained through sensor technology in a risk assessment process (e.g. for the purposes of renewals or extensions to cover) could potentially raise privacy and discrimination issues discussed above under the heading of "risk individualisation". The author is of the firm view that use of such data should be restricted and algorithms that use such data in risk assessment should be subject to audit along the lines discussed earlier.[83]

Furthermore, issues concerning the potential use of the data obtained from these devices could arise. UK GDPR gives the data subject a right to request the data controller to provide him/her with a copy of his/her personal data in a structured, commonly used and machine readable format and also request the data controller to transfer this data to another controller.[84] Therefore, insurers are under an obligation to provide data obtained from telematics devices or wearables with regard to the consumer in question to him/her or other insurance companies if requested by the consumer. That much is clear. A more difficult legal question will emerge if insurers attempt to claim ownership of such data with a view to exploiting it commercially by dictating in the insurance contract that the data obtained though such devices become their property. It is a debatable point whether ownership claims made in contract terms will be effective.[85] However, perhaps this is not a practical problem at this stage as we have not come across any standard insurance contract where insurers claiming ownership of such data.

It is also important to bear in mind that under the current data protection legislation there is no restriction on the ability of an insurer to use the real-time sensor data obtained from telematics devices or wearables for another purpose, eg in assessing risk for another product, as long as the individual is

[82] See text to notes 67–69 above and the discussion on the insurability problem.
[83] See text to notes 52–53.
[84] Article 20 of UK GDPR.
[85] It should be noted that UK courts have taken the view that data are not eligible to be subject of common law lien (*Your Response v Datateam Business Media* [2014] EWCA Civ 281, [2015] Q.B. 41) and no proprietary right is deemed to exist in the context of an email (*Fairstar Heavy Transport NV v Adkins* [2013] EWCA Civ 886, [2013] 2 C.L.C. 272) but with the developments in digital technology one should expect further legal developments in this area. It is worth mentioning that the Court of Appeal in *Computer Associates UK Ltd. v Software Incubator Ltd.* [2018] EWCA Civ 518, [2019] Bus. L.R. 522 held that software supplied to customers electronically and not on any tangible medium did not constitute "goods" within the meaning of regulation 2(1) of the Commercial Agents (Council Directive) Regulations 1993/3053 (this is currently on appeal to the Supreme Court).

given notice that such data will be used as part of risk assessment. It is, therefore, essential to devise guidance on the ethical use of sensor data by insurers along the lines discussed above.[86]

Last but not least, sensor data might introduce some novel vulnerabilities for the insured property. Imagine a situation where hackers use the network system that operates a home telematic device to gain access to a property in order to burgle it. It is possible that this might trigger penalties for the insurer under the data protection legislation.[87] But more significantly, if the resulting loss is not covered under the policy, the assured would be able to make a claim (for breach of contract and/or in tort) from the insurer who owns such a sensor device for failing to exercise due diligence to prevent such cyber attacks[88] leading to the loss not covered by the policy.[89] At first sight, these eventualities might seem far-fetched, but every disruptive new technology is capable of creating such novel problems and it is likely that such issues might be faced by insurers when the use of such technology becomes common in the market.

B. Creating Tailor-made Clauses to Deal with Risk Alteration by Utilising Sensor Data

In insurance law, it is open to a policyholder after attachment of the risk to alter the nature of the risk without the consent of the insurer.[90] In practice, however, risk control clauses are often employed by insurers to restrict this freedom. The main objective of a clause of this nature is to ensure that the risk is maintained by the assured at the same level agreed at the inception. Traditionally, warranties[91] are the most common risk control clause[92] used in insurance law.[93]

[86] See text to notes 52–54 above.

[87] The Information Commissioner Office under the UK GDPR and Data Protection Act 2018 can issue fines of up to 4 per cent of a company's annual global turnover, or £17.5 million (whichever is greater) for failure to secure data concerning individuals.

[88] In most policies, insurers exclude liability for any loss, damage liability or costs caused by inaccuracies in the data collected by the telematics device; but this kind of exclusion clause would not protect them against vulnerabilities in the system that enables access to hackers.

[89] This might create the need for insurers using such devices to consider purchasing cyber risk insurance cover.

[90] Chief Baron Pollock in *Baxendale v Harvey* [1859] 157 E.R. 913 (Ex. Ch.), 915–16, famously said: "If a person who insures his life goes up in a balloon, that does not vitiate his policy … .. A person who insures may light as many candles as he please[s] in his house, although each additional candle increases the danger of setting the house on fire."

[91] In a technical sense, an insurance warranty is an undertaking by the assured that "some particular thing shall or shall not be done", or that "some condition shall be fulfilled". Such warranties relate to facts after the attachment of the policy and are often known as future (or continuing) warranties. Some warranties, on the other hand, are undertakings whereby the assured "affirms or negatives the existence of a particular state of facts". A warranty of this nature is known as an affirmative warranty or a warranty that relates to a period before the attachment of the risk.

[92] Other risk control mechanisms often used are: (1) condition precedents to liability of the insurer (breach of such clauses either entitle the insurer to elect to discharge from the contract or prevent the assured from claiming for a particular loss); (2) suspensory provisions (also known as "clauses delimiting the risk"), which set out the circumstances in which the insurer is to be on risk; and (3) exclusion clauses.

[93] This is not the only function that an insurance warranty serves. Some warranties (i.e. affirmative warranties) intend to circumscribe the risk to which the insurer subscribes.

Telematics devices, which enable insurers to track the activities of the assured during the currency of the policy, could play a vital role in the quest of insurers to prevent risk alteration and determine the scope of the cover available. In contemporary policies, we are witnessing an increased use of such clauses especially in instances where the use of telematics is common. For example, in motor insurance policies, clauses are incorporated into the contracts, putting restrictions on the use of the insured car. In some policies it is stated that the insured car will not be driven more than X miles from the assured's home. Similarly, there might be a term stating that the insured car will not be driven at certain times of the day, eg between 8 a.m. and 10 a.m. or when it is in an unroadworthy condition. In some policies, there are terms where the assured warrants that the insured car will not be driven above the legal speed limits or when under the influence of alcohol or drugs. Some of the clauses are more draconian, allowing insurers to cancel the policy if the assured displays some kind of unacceptable driving behaviour.[94] Again, in instances where the insurers make use of home telematics, we often see warranties requiring the assured to keep various loss preventive devices (e.g. fire and burglar alarms) operative during the policy period. Needless to say, telematics devices make it possible to monitor compliance with this kind of term.

As long as such terms are written in plain language and transparent, it is difficult to see any reason as to why any restriction on their use should be imposed. Terms designed to prevent the assured from altering the risk have traditionally been incorporated into insurance contracts. For example, most assureds who took motor insurance policies in the 1920s would warrant that they would maintain the insured vehicle in an "efficient" or "roadworthy" condition, and an insurer who could prove that the vehicle was not in such a state would have had a defence to any claim arising out of an accident involving the insured vehicle.[95] So why should things be different if an

[94] See e.g. Condition 8, Unacceptable Driving Behaviour, in HughesDrive, an insurance policy which reads:

> "You and any additional drivers must observe the law at all times. Poor driving behaviour by any drivers (including driving at speeds which exceed the speed limit for the road on which the car is being driven) will affect your Driving Style Score. If the HughesDrive® App detects that your Driving Style Score is Red, a score less than zero, for any given week, you will receive notification. If, following this notification, you have a Red Driving Style Score for a further week, a final notice will be issued. Three consecutive weeks, or a total of five weekly scores which are Red during the life of your policy (including the week which prompted the original notification), will result in your policy being cancelled in accordance with the cancellation section of the private car policy booklet. In addition to this, we and/or the Insurer reserve the right at any time to provide you with seven days' notice and cancel your policy forthwith in the event that excess speed is detected. You have the right to appeal any decision made concerning your or any named driver's driving behaviour by contacting Hughes Insurance."
>
> A copy of the terms can be found at: "Terms & Conditions for HughesDrive® Telematics-based Motor Insurance Customers", https://www.hughesinsurance.co.uk/pdf/Telematics-Customer-Terms-Conditions.pdf (last accessed 15 August 2021).

[95] See e.g. *Jones v Provincial Insurance* (1929) 35 Ll. L. Rep. 135 (K.B.).

https://doi.org/10.1017/S0008197322000010 Published online by Cambridge University Press

assured today warrants that the insured vehicle would not be used at certain times of the day but an incident occurs and the telematics device confirms that the vehicle was in use during those times? Likewise, if a home insurance policy requires a fire alarm to be kept operative during the policy, and home telematics device informs the assured of a malfunction in his/her fire alarm system but s/he fails to take any action (i.e. fails to prevent a risk alteration), could any objection be raised for that particular assured not being able to recover for a loss caused by a fire?

Of course, this is not to say that validity of such terms could not be challenged under consumer protection legislation or regulations put in place to regulate the conduct of business of insurers. However, it is highly unlikely that terms used in the market concerning telematics devices or wearables will fall foul of such statutory provisions. For example, a warranty in a telematics motor policy that requires the assured not to drive the insured vehicle when under the influence of alcohol or drugs is unlikely to be viewed as unreasonable under Rule 2.5.1 of ICOBS,[96] affording a consumer assured a right of action for damages for breach of statutory duty under Section 138D of the FSMA 2000. In *Parker v National Union Mutual Insurance Society*,[97] a term that required the assured to provide all written details and documents requested by the insurer was not deemed to be contrary to the rules stated in ICOBS, as it could not be said that such term could give rise to a significant imbalance in the rights of parties, given that the assured alone possessed the information which might be required by the insurer. By analogy, it can be said that a term that puts restriction on the actions of the assured that are in his/her control is unlikely to give rise to a significant imbalance in the rights of parties. Even a term affording the right of the insurer to cancel the contract if the assured displays unacceptable driving behaviour as captured by a telematics device is unlikely to be viewed as "unreasonable" given that such a right usually crystallises only after the assured engages in a very unacceptable form of driving, and under such terms it is common to give a notice of cancellation to the assured and some time before cancellation becomes effective so that s/he can make alternative insurance arrangements.[98] For the sake of completeness, it should also be stressed that the author does not believe that the Consumer Rights Act (CRA) 2015 alters the position in favour of the assured, either. Even though section 62(1) of the 2015 Act provides that a term that is judged to be unfair will not be binding on consumers, section

[96] This Rule reads: "A firm must not seek to exclude or restrict, or rely on any exclusion or restriction of, any duty or liability it may have to a customer or other policyholder unless it is reasonable for it to do so and the duty or liability arises other than under the regulatory system."

[97] [2012] EWHC 2156 (Comm), [2013] Lloyd's Rep. I.R. 253.

[98] See e.g. the relevant term used in MYPOLICY, a commonly used telematics motor insurance policy, which can be found at: "Telematics Car Insurance Terms and Conditions", available at https://www.mypolicy.co.uk/media/1118/telematics_car_insurance_terms_and_conditions_v31pdf.pdf (last accessed 15 August 2021).

64(1) clearly states that a term of a consumer contract may not be assessed for fairness "if it specifies the main subject matter of the contract, or if the assessment concerns the appropriateness of the price payable under the contract by comparison with the goods, digital content or services supplied under it" as long as this term is "transparent and prominent to an average consumer".[99] When this section is read in conjunction with the explanatory notes that accompanied the EU legislation forming its origins[100] and the reasoning of English courts on the matter,[101] it is strongly arguable that any term in an insurance contract excluding or restricting the scope of the cover will not be subject to the fairness test referred to in section 62 (1) of the CRA 2015 as long as it is transparent and brought to the attention of an average consumer. This will certainly be true for a term in a consumer insurance motor policy that affords a remedy for the insurer in a case where telematics devices confirm unacceptable (dangerous) driving practice demonstrated by the consumer for a sustained period of time. Ultimately, insurance cover here is offered on the basis that the risk will be retained at a particular level (i.e. the assured will not alter the risk by engaging in unacceptable and/or dangerous driving behaviour during the currency of the policy).[102] If the assured acts contrary to this term, by virtue of the relevant term the process of cancellation commences. This is a very clear indication that the relevant clause is one that defines or circumcises the

[99] Section 64(2)–(5). When requested to construe the scope of this exception in the context of Article 4(2) of the Unfair Terms Council Directive 93/13/EEC (OJ 1993 L 95 p.29), the provision which forms the origins of section 64 of the CRA 2015, the Court of Justice of the European Union (CJEU) expressed the view in Judgment of 3 June 2010, *Caja de Ahorros y Monte de Piedad de Madrid*, C-484/08, EU:C:2010:309, at [32], that it is up to the national courts having jurisdiction, following a case by case examination, to form the view whether the relevant terms were drafted by the seller or supplier in plain, intelligible language. The Supreme Court, by making use of the flexibility afforded by the CJEU, adopted a broad interpretation of Article 4(2) of the Directive in *Office of Fair Trading v Abbey National plc* [2009] UKSC 6, [2010] 1 A.C. 696. There, the OFT challenged whether charges for unauthorised overdrafts fell within this exception. The Supreme Court held that the bank charges constituted part of the price or remuneration for the bank services provided. On that basis, provided they were in plain and intelligible language, the banks' overdraft charges could not be assessed for fairness. There is little doubt that the reasoning holds true in the context of Section 64 of the CRA 2015 which does not alter the exceptions in any significant manner apart from requiring that the term is brought to the consumer's attention in such a way that an average consumer would be aware of the term (in addition to transparency requirement). It is fair to say that the CRA 2015 supports a market-led approach which expects consumers to be self-reliant and protect their own interest.

[100] This section replaces relevant parts of the Unfair Terms in Consumer Contracts Regulations 1999, which was designed to implement the EEC Unfair Consumer Contract Terms Directive 93/13/EEC, into English law. Recital 19 of the Directive 93/13/EEC, stated: "in insurance contracts, the terms which clearly define or circumcise the insured risk and the insurer's liability shall not be subject to such assessment [fairness] since these restrictions are taken into account in calculating the premium paid by the consumer."

[101] See in particular *Parker v National Union Mutual Insurance Society* [2012] EWHC 2156 (Comm). Teare J. held that a term that puts the assured under an obligation to do things which are in his/her control could not be struck down by the Unfair Terms in Consumer Regulations 1999 (which forms the basis of the relevant sections of the Consumer Rights Act 2015). See also *Office of Fair Trading v Abbey National plc* [2009] UKSC 6, [2010] 1 A.C. 696.

[102] In the context of insurance law, such terms are invariably regarded as essential terms of the contract. See e.g. *Simpson SS Co. Ltd. v Premier Underwriting Association Ltd.* (1905) Com. Cas. 198 and *Farr v Motor Traders' Mutual Insurance Society Ltd.* [1920] 3 K.B. 669.

insured risk and ultimately the liability of the insurer so it is highly unlikely that it needs to be subjected to the "fairness" test stipulated in section 62.[103]

Leaving consumer protection legislation aside, it should be noted that general insurance rules might provide some degree of protection to assureds who might face restrictions imposed by telematics insurance policies. Imagine for example, a telematics home insurance policy which requires the assured with a warranty to keep the burglar alarm in an operative condition during the policy period. A defect in the burglar alarm is identified by telematics and although the assured is informed no corrective action is taken. A few days later, the insured property is damaged as a result of a storm affecting the region. Normally, in case of breach of an insurance warranty, the cover is suspended until the breach is remedied,[104] but section 11 of the IA 2015 stipulates that the assured will be indemnified for a loss occurring at a time when a warranty (or term) is not complied with if (1) compliance with the warranty (or term) in question would tend to reduce the risk of loss of a particular kind, loss at a particular location or loss at a particular time; and (2) the assured demonstrates that non-compliance with the warranty (or term) could not have increased the risk of the loss which actually occurred in the circumstances in which it occurred.[105] To seek refuge in this section, the assured in the light of the loss arising must first establish that the warranty (or term) that is breached is intended to reduce the risk of loss of a particular type or at a particular location or at a particular time. The test that is introduced here is an objective one and it essentially attempts to identify whether compliance with the warranty (or term) is thought to reduce the chances of the particular type of loss being suffered. Turning to the example above, the assured would possibly be able to establish that the relevant warranty would objectively tend to reduce the risk of break-in (and related events such as arson and vandalism). This will mean that the insurer's liability in respect of break-in would be suspended during the period of breach. If, however, a loss arises as a result of another peril, such as a storm, that is not connected to unauthorised entry into the premises, that loss will be covered as the assured in all probability will be able to demonstrate that non-compliance with the warranty (i.e. burglar alarm not being in operation) could not have increased the risk of loss caused by storm.[106]

[103] This is an outcome which is in line with the view expressed by the CJEU in Judgment of 30 April 2014, *Kásler*, C-26/13, EU:C:2014:282, at [49], to the effect that a term in a contract that is not subject to "fairness" test is one that lays down "the essential obligations of the contract and, as such, characterise it".

[104] Insurance Act (IA) 2015, s. 10.

[105] It is not possible for insurers to contract out of this provision in consumer insurance policies (IA 2015, s. 15). However, in commercial insurance policies, it is possible to contract out of these provisions subject to transparency safeguards as set out in section 17.

[106] However, difficulties can arise in some cases. E.g., in the scenario discussed above, assume that the cause of the loss is fire. The insurer in that case might potentially argue that a burglar alarm that is sensitive to motion might have detected the fire spreading and alerted the residents and possibly emergency

However, one should not lose sight of the fact that section 11 of the IA 2015 does not apply to a warranty (or term) that is designed to describe the limits of the cover as a whole. Put differently, if a warranty (or term) has the effect of limiting the scope of cover generally as opposed to limiting the effect of a breach in relation to a specific risk, the assured will not be able to rely on section 11 if a loss occurs during the period of breach. This would mean that if a telematics motor policy imposes a warranty to the effect that the insured car should not be driven X miles from the assured's home, the assured will not be able to recover for a loss that arises beyond those limits.[107] By a similar token, a telematics motor policy that stipulates that the insured car would not be used at certain times of the day will not respond to a claim that arises from a loss occurring during those hours. Of course, it is inevitable that boundary disputes will arise. Imagine that in a telematics motor insurance policy there is a warranty or condition precedent requiring the insured vehicle to be kept "in a roadworthy condition at all times". Also imagine that the assured drives the car when headlights are not working during the daytime and a collision occurs as a result of another driver hitting the insured car from behind. The assured could plausibly argue that the term was designed to reduce the risk of loss when the car is driven at night with no functioning headlights so the breach here (driving when headlights not fully functioning during daytime) could not have increased the risk of loss in the circumstances in which it occurred. Equally, it is plausible for the insurer to argue that this is a risk-defining clause and it imposes a restriction (driving only when roadworthy) that relates to the risk as a whole, so section 11 is not relevant here. It is the author's opinion that the latter argument is more palatable given that the condition that the insured vehicle should be kept at during the currency of the policy is a matter which goes to the heart of risk definition. Accordingly, it is very likely that the assured's cover will remain suspended during the period when the insured vehicle was used when headlights were not functioning.

It needs to be emphasised that cancellation clauses do not come under the scope of section 11. Hence, it is no surprise to see most telematics motor insurance providers opting to employ cancellation clauses that allow them to cancel the policy if it is recorded that the insured driver has engaged in dangerous driving patterns (e.g. repeatedly driving over speed limits). However, there is convincing judicial authority to the effect that

services, so non-compliance in this case did in fact increase the risk of the loss which actually occurred in the circumstances in which it occurred. This is certainly a plausible argument that insurers can take. Therefore, one cannot help thinking that one effect of section 11 will serve more than introducing causation by the back door! See B. Rix, "General Reflections on the Law Reform" in M. Clarke and B. Soyer (eds.), *The Insurance Act 2015* (Oxford 2017), 120–21.

[107] See the judgment of the Queensland Supreme Court in *Stapleton v NTI Ltd.* [2002] Q.D.C. 204 that considers the issue from the perspective of a similar legislation.

in cases where the insurer is entitled to exercise discretion under the policy on the basis of information obtained (e.g. when exercising a right of cancellation), the insurer is expected to exercise this discretion in a reasonable fashion, without arbitrariness, capriciousness or perversity.[108] The legal basis of this qualification remains uncertain. Some commentators associate it with the duty of good faith,[109] although the precise ambit of the application of good faith principle in this connection is far from being clear.[110] Assuming that the continuing duty of good faith has a role to play here, it is likely that it will require the insurer that obtains information from a telematics device about the driving behaviour of the assured not to act dishonestly, improperly, capriciously or arbitrarily.[111] However, it should be borne in mind that most cancellation clauses used in telematics motor insurance policies stipulate that, when exercising the right of cancellation, the insurance company must notify the assured of the reasons for cancelling and also explain those reasons. This is a clear sign that insurers are well aware of the fact that their cancellation right is subject to various limitations imposed by law, and it is therefore unlikely that they would act in an arbitrary fashion when exercising a right of cancellation after having obtained data from telematics indicating unreasonable driving behaviour of the assured.

It should, finally, be noted that under the Road Traffic Act 1988, the insurer could be prevented from relying on some of the risk control clauses that might appear in a telematics motor insurance policy to deny cover against third parties. Section 148(2) of the Road Traffic Act 1988, *inter alia*, stipulates that a third-party liability insurer cannot rely on matters such as the age, physical condition, or mental condition of persons driving the vehicle, the condition of the car, or the time at which or the areas within which the vehicle is used. That means that a warranty that requires the insured car not to be driven at certain times or outside a geographical limit cannot be used to deny liability to third parties if the insured vehicle is involved in an accident during those times or outside those geographical limits. The same is true in relation to a term that requires the car to be driven in a "roadworthy" condition or a term preventing the insured to drive the insured car when under the influence of drugs or alcohol. In those circumstances, an insurer who pays out a third-party claim could seek to recover this sum from the assured under section 148(4) of the Road Traffic Act 1988.

[108] See e.g. *Groom v Crocker* [1939] 1 K.B. 194 (C.A.), 203 (Sir Wilfrid Green M.R.); *Cox v Bankside Members Agency Ltd.* [1995] C.L.C. 671 (C.A.), 680 (Sir Thomas Bingham M.R.).

[109] Soyer and Tettenborn, "Mapping (Utmost) Good Faith", 625–26.

[110] E.g. Pill L.J. in *Drake Insurance Plc v Provident Insurance Plc* [2003] EWCA Civ 1834, [2004] Q.B. 601, at [177]–[178], was adamant that continuing duty of good faith can be breached by an insurer even in the absence of fraud.

[111] See also *Socimer International Bank Ltd. v Standard Bank London Ltd.* [2008] EWCA Civ 116, [2008] 1 Lloyd's Rep. 558 and *Paragon Finance Plc v Nash* [2001] EWCA Civ 1466, [2002] 1 W.L.R. 685.

IV. Concluding Remarks

Big data analytics and artificial intelligence are rapidly changing the way insurers run their businesses. They particularly assist insurers (1) to individualise the risk assessment process at a granular level; and (2) to customise insurance products they offer to the public. It is argued in this article that consumers are not necessarily in a worse position in terms of (2), as consumer legislation and general principles of insurance law could ensure that the use of algorithms and artificial intelligence do not provide any unfair advantage to insurers.[112] However, it has been also asserted that uncontrolled use of data analytics and algorithms in the process of risk assessment could create various difficulties for consumers since the existing legislation, in particular data protection legislation, could not provide the required degree of protection for consumers. It has been illustrated that there are legitimate concerns as to whether the privacy of consumers can be adequately protected. It is also possible that the use of algorithms might lead to indirect discrimination in some cases against some consumers, as such programmes are designed to find linkages between input data and target invariables irrespective of the nature of these linkages. There is also the potential of errors in the data collection or data analysis that could create unforeseen consequences for some assureds. Finally, it has been illustrated that a granular risk assessment might create insurability problems for some group of people (especially those who have genetic or chronic health problems). This is an issue that policy-makers need to consider seriously, as it might be necessary to show solidarity and preclude the use of certain types of data from the risk assessment process.

The main conclusion emerging from the article is that it is essential to consider regulating further the use of algorithms and big data analytics especially in the process of risk assessment. The issues that need to be considered carefully by policy-makers have been highlighted in this article. Also, it has been suggested that there is a need to establish a new agency that can undertake the task of running random audits to ensure that the algorithms used are within the parameters set.

This technology presents great opportunities for insurers. And, it is certainly vital that the right balance is struck in regulating a new area of development, since over- regulation could prevent this technology from achieving its full potential. It is evident that some degree of regulation beyond the current legislation of data protection is required so that this technology is used in a fair and transparent fashion in the risk assessment process. It is hoped that the insurance sector recognises this, and even perhaps plays an active role in shaping the regulatory framework in this area.

[112] This remains the case as long as real-time data obtained by sensors is not used as part of any risk assessment for renewals and extensions.