PINNACLE
ACTUARIAL RESOURCES, INC.
Commitment Beyond Numbers

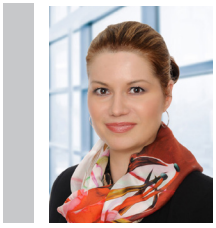
Monograph

pinnacleactuaries.com

Artificial Intelligence – Welcome Opportunity or Inescapable Challenge for Insurers?

Radost Roumenova Wenman, FCAS, MAAA, CSPA

ABOUT THE AUTHOR



Radost Roumenova Wenman
FCAS, MAAA, CSPA

Radost Roumenova Wenman is a Consulting Actuary with Pinnacle Actuarial Resources, Inc. in the San Francisco, California office. She holds a Master of Science degree in Statistics and a Bachelor of Science degree in Mathematics from Stanford University.

Ms. Wenman has over 12 years of experience in the Property and Casualty Insurance arena, focusing on pricing and product development. In this role, Ms. Wenman has developed homeowners and private passenger auto pricing solutions through the design and implementation of advanced predictive models.

Ms. Wenman serves the Casualty Actuarial Society (CAS) as a member of the CAS Actuarial Review Committee and member of the iCAS Education Committee.

For more information on this topic, contact Radost at (415) 692-0260 or rwenman@pinnacleactuaries.com

The proliferation of big data and artificial intelligence (AI) impacts practically every human enterprise and endeavor. The insurance industry is certainly no different, having historically thrived on developments in data, data analytics, AI and other information technologies. Insurance companies are taking advantage of the digital transformation to automate claims management processes, improve operational efficiencies, and increase the quality of service they deliver to customers with personalized marketing and recommendations. The ongoing race to conquer volumes of heterogeneous data and wring every bit of informational value out of raw intelligence will mean growing opportunities and inevitable challenges for insurers, the insured and most participants in the insurance sector.

What we mean by big data and AI

Big data, the diversity and quantity of data available to insurers, combined with increased computing power and data storage capacity, has begun to disrupt the landscape of insurance analytics and applications in profound ways. Big data is a continually evolving concept characterized by the "Five Vs:" volume, velocity, variety, value and veracity. An increasingly complex ecosystem of vast amounts of diverse data (volume and variety) collected at a fast rate (velocity) has persuaded enterprises to implement sophisticated analytical tools to help them draw actionable insights (value) from reams of reliable data (veracity).

KEY POINT

An increasingly complex ecosystem of vast amounts of diverse data collected at a fast rate has persuaded enterprises to implement sophisticated analytical tools to help draw actionable insights from reams of reliable data.

Perhaps the most common example of a big data insurance application is the collection of data via telematics. Automobile insurers use data to perform spatiotemporal analysis of policyholder driving behavior and associated risk. Insurers can use telematics data to price risk more accurately and offer additional services, such as promoting safer driving practices or indicating locations that exhibit high frequency of accidents.

Artificial intelligence is broadly defined as the ability of machines to solve problems or perform complicated, sometimes human tasks–self-driving cars and computers playing chess, for example. Machine learning (a term often used interchangeably with AI) is

a subset of AI that encompasses a wide range of sophisticated computer algorithms that rely on big data to enable machines to find patterns, learn and predict.

The insurance sector is demonstrating great interest in leveraging AI and machine learning. According to a recent market research report, the insurance industry in the Unites States increased AI investments 83% in 2018, for a total outlay amounting to almost $259 million. Those numbers are expected to reach $2.6 billion by 2025.[1]

Machine learning tools could benefit insurers in the detection and interception of insurance fraud. In the underwriting process, some customers intentionally misrepresent information, committing soft fraud. At the claims submission stage, others may attempt to overestimate loss amounts or possibly file fraudulent claims for fake accidents, committing hard fraud.

Historically, fraud detection has involved combining subject matter expertise with supervised learning to identify and profile potential fraudsters. These supervised techniques are fraught with challenges, however. Supervised techniques are often time-consuming, difficult to apply with imbalanced data, inefficient with organized crime or with patterns that are constantly evolving.

Unsupervised methods, such as link-and-graph analysis and fuzzy clustering can be useful because they do not rely on predefined labels ("fraud" vs. "not fraud"). Rather, these tools search for patterns in customer behavior and visualize the connections (or, links) between various types of information contained in a transaction – customers, times, locations and service providers. The goal is to uncover potential fraud rings within a network of involved, and sometimes seemingly unrelated, entities.

Speech recognition algorithms that perform voice analysis of customer calls also show promise. Speech recognition can be used in identity authentication and the detection of stress. Speech recognition applications have been suggested as an important part of the next generation of fraud analytics for call centers.

AI and machine learning have promise in other sectors of the insurance-value chain. That promise includes enhancing customer experience with personalized product recommendations, claims settlement process automation, subrogation and litigation, direct marketing and customer retention. Insurers may be aware of the benefits they can reap from leveraging AI and machine learning, but many remain uncertain about how to best maximize results from those technologies.

The reason for their hesitance may be the uncertainty and risks associated with AI algorithms. A new report, "Taking control: artificial intelligence and insurance," (Maull et al., 2019) commissioned by Lloyd's and published in collaboration with the University of Surrey, attempts to explain the insurance industry's careful adoption of some new technologies. In its report, Lloyd's identifies trust and transparency, ethics, security and liability as the most urgent risks facing adoption and contributors to a recent rise in skepticism about the implications of this new digital environment.

Understanding (and misunderstanding) AI

There is a cloud of concern shrouding the use of AI in a number of industries. This may originate from a perceived lack of transparency which has diminished societal trust in the technology. AI systems are sometimes considered "black boxes" with mechanisms of operation and decision-making that can be difficult to explain, sometimes even by the experts who created these systems. The *Harvard Journal of Law and Technology* (Bathaee, 2018) describes the complexity of AI algorithms:

> "…may be based on patterns that we as humans cannot perceive, which means understanding the AI may be akin to understanding another highly intelligent species – one with entirely different senses and powers of perception. This also means that little can be inferred about the intent or conduct of the humans that created or deployed the AI, since even they may not be able to foresee what solutions the AI will reach or what decisions it will make." (p. 5)

The challenge of reducing an AI system to a crisp set of rules is evident if we account for the intricate structure and interdependence among AI units. Deep neural networks (DNNs) and support vector machines (SVMs) offer an instructive example in this instance. DNNs and SVMs are techniques typically

1 "United States Artificial Intelligence (AI) in Insurance Industry Databook Series (2016-2025) - AI Spending with 15+ KPIs, Market Size and Forecast Across 6+ Application Segments, AI Domains, and Technology," (2019). TechInsights360.

used for the analysis of unstructured data such as image, text and audio files. Insurance companies can utilize these advanced methods to estimate cost of claims based on images as well as improve customer experience and satisfaction through analysis of customer comments, captured either in text or audio. Parametric insurance, an index-based insurance, is an emerging risk-transfer mechanism. Parametric insurance is a predetermined payment contingent on some triggering event (e.g., earthquake) that utilizes DNN and SVM techniques to analyze satellite images and create a wide range of disaster indicators.

DNN architecture consists of multiple layers of thousands or hundreds of thousands of interconnected units, called neurons, that continuously and iteratively exchange information. Neurons optimize the algorithm and work together to crank out patterns and predictions. As the *Harvard Journal of Law and Technology* report explains, "one cannot in most cases point to any neuron or group of neurons to determine what the system found interesting or important. Its power comes from 'connectionism,' the notion that a large number of simple computational units can together perform computationally sophisticated tasks." (p. 15)

SVMs also exhibit complex structures and underlying computations that contribute to society's perception that AI is a black box. SVMs have proven their utility with various types of data, particularly highly dimensional data containing hundreds and thousands of variables. The goal of the model is to discover geometric patterns and relationships among the multiple dimensions that are difficult to perceive and visualize by the human brain.

Bathaee illustrates these difficulties by asking the reader to imagine using weight and height data to make predictions about a person's gender. Initially, this is not difficult for humans to visualize: a plot of weight and height values on a two-dimensional graph with lines (or curves) between points that most effectively separate males from females. A task made relatively simple when there are only two or three variables. If we introduce more variables to the model, however, "the human mind is unable to visualize what that dividing line (curve) looks like. Human brains simply cannot visually process high dimensionality. An AI that uses an SVM to process dozens or perhaps hundreds of variables would thus be a black box to humans because of the dimensionality of the model." (p. 17)

The increasing complexity and opacity of AI systems have fostered human beings' anecdotal mistrust of cognitive algorithms. It should not be so. AI has tremendous societal and commercial benefit with great potential value for consumers, science, healthcare and for businesses in all industries, including insurance. To take advantage and win trust of consumers, businesses and users of AI-enabled algorithms need to provide clear interpretations of how their models operate and make decisions.

The rise of interpretability: From black box to glass box

Lloyd's 2019 report highlights an encouraging trend in the AI community. While developers continue to focus on improving and building highly flexible models that can extract patterns, predict and classify beyond the capacity of the human mind, many remain dedicated to ensuring that these models are explainable and free of sample and prejudice bias or intentional harm. Understanding the potential for misuse and abuse of AI, developers have commendably focused on expanding explainable models of AI. These models (often abbreviated "XAI" for Explainable AI) are appropriately termed "glass box" models in contrast to the black box perception of historical AI systems.

"Explanation Methods in Deep Learning – Users, Values, Concerns, and Challenges," (Ras, Haselager, van Gerven, 2018) provides an exemplary list of methodologies currently being explored with an aim "to strengthen the confidence and trust of users that

the system is not (or will not be) conflicting with their values, i.e., that it does not violate fairness or neutrality" (p. 5). The authors examined historical and contemporary trends to categorize XAI explanation methods into three groups: rule-extraction methods, attribution methods and intrinsic methods.

Rule-extraction methods best resemble the mechanism of decision trees. In decision trees, datasets decompose into increasingly smaller subsets. Each branch, or layer, is determined by one or more of the input features (the variables that describe the data samples). The goal of these techniques is to translate the AI system into easily comprehensible "if-then" rules that describe the logic of the AI decision-making process. "In terms of explanatory power, rule-extraction methods can 1) validate whether the network is working as expected in terms of overall logic flow, and 2) explain which aspects of the input data had an effect that lead to the specific output." (p. 7)

Attribution methods, also known as influence methods, can assist in digesting the schema of an AI model by quantifying importance of various inputs. The underlying goal is to vary input values and sequentially measure resulting changes in model performance. Attribution methods are extremely flexible because they can handle various types of input data including text and images. These techniques can also construct a visualization map (or salience mapping) that shows which data components play the most significant role in shaping the model output.

Rule extraction and attribution methods interpret AI systems post hoc with external processes. Intrinsic methods, on the other hand and as the name suggests, operate by utilizing internal AI system processes (e.g., the loss function or operation between DNN layers). These methods improve interpretability, or the ability to explain AI systems' output and decisions they make, by integrating semantic information from human descriptions. Interpretability of the AI architecture becomes a function of the AI model and internally guides the learning process. Importantly, researchers have shown that intrinsic models can train an AI algorithm with adversarial data, trace the errors back to the specific part of the AI that made the error and determine whether that data was indeed adversarial.

Adversarial data is especially pernicious for its malicious intent to deceive the model and lead to conclusions that purposely harm people. A common example of machine learning models infected with adversarial data is self-driving cars causing a crash because the physical driving environment was modified (e.g., stickers on the road or stop signs that were altered to speed limit signs). Fortunately, these examples have been demonstrated only in experimental settings and not the real world, but they underscore the need for AI systems that are resistant to tempering and malicious intent.

Recently, Harvard University and Massachusetts Institute of Technology (MIT) researchers studied a scenario, captured in Science magazine, from the field of medical insurance fraud. They showed how

an image of a skin mole can be slightly modified to force the machine learning image recognition software to classify it as malignant instead of benign and recommend treatment. In this hypothetical instance, a health insurance company would be required to make a payout to the health care provider, unaware of the underlying scam.[2]

Ethics, public trust and the law

The aforementioned methods for enhancing interpretability offer a promising future for AI applications and the attendant effort to solidify societal trust. We must acknowledge, however, that an AI system may behave adversely because of unwanted biases in the data rather than the design of the algorithm itself. AI and machine learning methods behave "intelligently" only to the extent that the data used for knowledge extraction lacks selection biases and can generalize well and across all situations. Unethically selected data is a recipe for disaster and will produce flawed modeling results.

In the Lloyd's report, Maull et al. (2019) cite two recent and problematic uses of data in AI applications.

In 2018, Amazon discovered that an employee recruitment tool it had been testing was exhibiting gender bias. The tool consistently downgraded job applications that contained the word "women's" (as in "women's college" or "women's chess club"). It was determined that the AI algorithm was fed data consisting of 10 years of employment applications submitted mostly by male candidates. Amazon attempted to remove the gender-biased data but scrapped the project entirely due to concerns with other potential biases.

In 2016, investigative news organization ProPublica asserted in its series "Machine Bias" that an AI software used by some U.S. court systems for risk assessment and predicting future crime was biased against people of color. ProPublica claimed [that] "In forecasting who would reoffend, the algorithm was flagging black defendants as future criminals almost twice the rate as white defendants, who were being mislabeled as low risk more often than their black counterparts." The controversy seemed to be a realization of concerns expressed by U.S. Attorney General Eric Holder in 2014: "Although these measures were crafted with the best of intentions, I am concerned that they inadvertently undermine our efforts to ensure individualized and equal justice. They may exacerbate unwarranted and unjust disparities that are already far too common in our criminal justice system and in our society."

Ethical and trust concerns are only a few of the implications of increased—and increasing—prevalence of AI and machine learning. The new and fast-developing technology has the potential to radically expand other risks such as cybercrime and legal uncertainty.

Many cybersecurity experts believe that AI can be mobilized to help identify and thwart cyber threats and attacks. Others, however, fear that these powerful algorithms have the potential to wreak havoc on businesses and individuals should they be used for criminal ends. One nefarious use of AI technology allows hackers to devise more sophisticated spear phishing messages to gain access to private data or invade computer systems.

What it means for the insurance industry

The increasing diversity of digital risks will likely create new legal uncertainties, new legislation and inevitable litigation over liability and accountability when an AI-powered system fails to operate properly or causes damage to property or human life. Internet of things (IoT) devices, including connected cars, smartphones, drones, household appliances, medical devices, etc., all rely on machine learning algorithms to make decisions. It will become necessary to establish a legal framework that will "bring together a much broader constituency than those who created these technologies." (Maull et al., p. 28)

The 2019 Lloyd's report discusses legal challenges to AI systems in general but also identifies a series of specific insurance lines of business that will likely experience the greatest impact from these challenges: product liability, third-party motor liability, cyber, fidelity, medical malpractice and political risks.

Product liability and product recall can be particularly impacted by malfunctioning AI systems. Software malfunctioning after encountering code with which it is unfamiliar, for example. There may also be an instance when various AI components miscommunicate and negatively impact a product's design or manufacture. "Product manufacturers, AI designers, and AI purchasers could be allocated fault by courts in liability cases. This could mean that in the future, companies might buy more contractual warranties,

2 Finlayson, S., Bowers, J., Ito, J., Zittrain, J., Beam, A., & Kohane, I. (2019) "Adversarial attacks on medical machine learning." *Science 22,* 363 (6433), pp. 1287-1289.

indemnities and limitations to control AI liability risk." (Maull et al., 2019, p. 6)

Two recent Boeing 737 MAX8 crashes are a chilling example of an AI system gone awry. It is believed that the airplanes' angle of attack sensors, which provide critical feedback on tilt of the aircraft (the degree of up or down orientation), sent incorrect data to the plane's "maneuvering characteristics augmentation system" AI mechanism. The AI system overrode pilot control of the plane possibly because of the incorrect information, and prevented the pilots from correcting and controlling the aircraft.

Significant challenges are also expected in the third-party motor liability space. Currently, vehicle drivers and insurance companies share responsibility for losses. With the much-expected shift toward autonomous vehicles, liability may transfer to car manufacturers and AI software suppliers. "As a result, the market for third-party liability cover may reduce significantly in some territories, perhaps with a related increase in the demand for manufacturers' product liability insurance." (Maull et al., 2019, p. 37)

Increasing sophistication of human-like chat bots and "deep fakes" will make it almost impossible to tell humans and AI apart in some instances. A deep fake is altered video or photographic content, enabled by AI-technology, of people, things and events that either do not exist or did not occur. "This could make it easier to carry out phishing scams, and on a wider scale, as well as harder to detect them."(Maull et al., 2019, p 6) These types of security risks could pose significant difficulties for both cyber and fidelity insurers. The concept of insurable event and the applicable coverages, for example, will have to be carefully redefined.

Challenges associated with chat bot technology were highlighted in a 2019 Delta Airlines' lawsuit against chat bot provider [24]7.ai, Inc. Delta alleged that [24]7.ai did not install necessary cybersecurity safeguards to protect Delta customers' personal data, resulting in a 2017 breach that affected 825,000 customers. Delta claimed that [24]7.ai failed to employ basic security measures such as multilevel authentication controls and prohibiting its workers from using the same login credentials. As a result, Delta claimed, hackers were able to modify the chat bot source code and gain access to Delta customers' personal and financial data.[3]

One emerging and successful application of AI is in the field of medical imaging and diagnostics. It has been shown that AI can, in some instances, outperform the accuracy of well-trained physicians. Although these applications have proven useful as a personal assistant to medical professionals, physicians are still naturally concerned about treating their patients using input from a machine, and what that may mean for malpractice claims. "Where liability can be clearly attributed to the AI, this could be easily excluded under a medical malpractice policy. However, if AI is used as an aid, or is used negligently i.e. not used or set up correctly, liability and proximate cause determination could become complex." (Maull et al., 2019, p. 39)

In the spectrum of political risks, Maull at al. assert that "…the [weaponization] of AI could take many forms including corruption of data, biased data selection, and the illegal use of data leading to various outcomes including propaganda, behavioral change and deception. From a political risk coverage perspective, AI might contribute to creating new or exacerbating existing political events such as expropriation, wars, acts of terrorism, civil disturbances and other forms of political violence in both developing and developed markets." (Maull et al., 2019, pp. 24, 41).

The future is now

AI capabilities will continue to grow and opportunities for their use continue to expand. The insurance industry must also continue assessing its place in the digital spectrum and taking advantage of the opportunities that AI promises. Companies able to access big data, transform it into a profitable investment and manage a bumpy road toward analytical superiority will likely create a fundamental shift in the insurance market. More reluctant companies, those unable to sustain or take advantage of the big data and AI, risk becoming less relevant.

At the same time, insurers must be cognizant of the associated risks and respond to the changing technological environment by developing new products and services to better meet the needs of their customers and society in general. It will be impossible to escape AI; it is far smarter for insurers to continue to embrace it, make it work for them and their customers by recognizing and mitigating all associated risks.

3 Stupp, C. (2019, August 16). Delta Sues Chatbot Provider Over 2017 Breach. The Wall Street Journal, Retrieved from www.wsj.com.

In his posthumously published book, "Brief Answers to the Big Questions," theoretical physicist Stephen Hawking offered an ominous warning about AI: "It will either be the best thing that's ever happened to us, or it will be the worst thing. If we're not careful, it very well may be the last thing…Whereas the short-term impact of AI depends on who controls it, the long-term impact depends on whether it can be controlled at all."

As dark a prospect as that may seem, technology, according to Hawking, is a product of our collective humanity and wisdom: "Whenever we make a great new leap, such as the Moon landings, we elevate humanity, bring people and nations together, usher in new discoveries and new technologies."

Hawking's faith is hopeful, but tempered - technology has to be applied responsibly. AI must be managed properly wherever and whenever it is used. For the insurance field, ready or not, that time is now.

References

Bathaee, Y. (2018).The Artificial Intelligence Black Box and the Failure of Intent and Causation. Harvard Journal of Law & Technology, pp. 890-934.

Finlayson, S. G., Bowers, J. D., Ito, J., Zittrain, J. L., Beam, A.L., & Kohane, I. (2019). Adversarial attacks on medical machine learning. Science 22, 363 (6433), pp. 1287-1289.

Maull, R., Collomosse, J., Brewer, S., Bordon, A., Jones, K., & Breeze, J. (2019). Taking control: artificial intelligence and insurance. Lloyd's and University of Surrey.

Ras, G., Haselager, P. & van Gerven, M. (2018). Explanation Methods in Deep Learning: Users, Values, Concerns and Challenges. Title of chapter in Jair Escalante, H., Escalera, S., Guyon, I., Baró, X., Güçlütürk, Y., Güçlü, U., & van Gerven, M.A.J. (Eds.) Explainable and Interpretable Models in Computer Vision and Machine Learning, New York City, Springer.

Stupp, C. (2019, August 16). Delta Sues Chatbot Provider Over 2017 Breach. The Wall Street Journal, Retrieved from www.wsj.com.

"United States Artificial Intelligence (AI) in Insurance Industry Databook Series (2016-2025) - AI Spending with 15+ KPIs, Market Size and Forecast Across 6+ Application Segments, AI Domains, and Technology," (2019). TechInsights360.

ABOUT PINNACLE

Pinnacle Actuarial Resources, Inc. is an independent, full-service actuarial firm that focuses on the property/casualty insurance industry. Our home office is located in Bloomington, Ill., with additional offices in Atlanta, Chicago and San Francisco.

Our *Commitment Beyond Numbers* philosophy encompasses all of who we are and what we do. It drives us to do whatever it takes to help our clients address their risks, understand the challenges they face and find the right solutions to meet their goals.

PINNACLE
ACTUARIAL RESOURCES, INC.

CONTACT INFO:

Radost Roumenova Wenman
FCAS, MAAA, CSPA
(415) 692-0260
rwenman@pinnacleactuaries.com

Contact us or visit pinnacleactuaries.com to discover more about how we can demonstrate our commitment to meeting your business needs.

Commitment Beyond Numbers.

The operative word is 'commitment.'

Pinnacle is committed to our employees, to our profession, to our community, and most importantly, to you.

A full-service actuarial firm, Pinnacle's mission is simple: We're here to provide professional expertise and superior customer service. Through data-driven research backed by clear communication, we work hard to ensure that our work is of substantial value to your business. You can trust Pinnacle's commitment to work with you to look beyond today's numbers in planning for tomorrow.

Commitment Beyond Numbers

PINNACLE
ACTUARIAL RESOURCES, INC.

Alternative Markets | Enterprise Risk Management | Legislative Costing | Litigation Support | Loss Reserving | Predictive Analytics | Pricing and Product Management | Reinsurance

pinnacleactuaries.com