



CLM 2020 Focus: Cannabis, Environmental, Insurance Fraud,  
Property, Subrogation, Claims & Litigation  
November 3-5, 2020

**“Danger, Danger Will Robinson, Navigating Fraud in the New AI Terrain”**

**I. What is Artificial Intelligence**

“Artificial intelligence is either the best thing or worst thing to happen to humanity.” Stephen Hawking

The term, “AI” is a confusing cacophony of conflicting concepts. The English Oxford Living Dictionary defines Artificial Intelligence as follows:

The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.

AI is evolving rapidly, as is the understanding and definition of the term. While many consider machine learning and algorithmic computations (which have existed for many years) as AI, some of the world’s most brilliant minds conceived Artificial Intelligence as existing only under the following circumstances:

- Can the robot/computer convince a human that they are communicating with another human? **Alan Turing (1950)**
- Can a robot completely automate economically important jobs? **Nils Nilsson (2005)**
- Can a robot walk into an unfamiliar house and make a cup of coffee? **Steve Wozniak (2007)**
- Can a robot enroll in university, take classes and get its degree, just like a human would? **Ben Goertzel (2012)**

While we clearly are not there yet, “AI” in its broadest definition is part and parcel of our everyday lives. We have smart phones, smart watches, self-driving cars, Siri, Google Earth, Uber, and AirBnB, to name a few. As such, for purposes of this presentation, we will be using

the widest of definitions: AI is the broad discipline of creating intelligent machines that can simulate human learning. Within that broad definition are the following concepts:

- Machine Learning (ML) - computer models that follow instructions and recognize patterns – i.e., face recognition
- Deep Learning (DL) - computer systems that apply machine learning without express instructions and can learn and identify patterns on its own – i.e., self-driving vehicles, Waze or traffic alerts
- Artificial Neural Networks (ANN) - models of human neural networks that are designed to help computers learn – i.e., <https://quickdraw.withgoogle.com> and Sketch RNN <https://www.theverge.com/2017/4/13/15284448/google-ai-draw-doodles-sketch-rnn>
- Natural Language Processing (NLP) - systems that can understand language – i.e., email filters, search results, predictive text
- Automated Speech Recognition (ASR) - the use of computer hardware and software-based techniques to identify and process human voice – i.e., Siri

## **II. The Use of Artificial Intelligence in the Insurance Industry**

While certainly at a slower pace, the use of AI is becoming commonplace in the insurance world touching all aspects of the industry from sales and marketing, to underwriting and actuarial calculations, to claims and operational processes.

### **A. Sales and Customer Service:**

For example, in the sales and marketing areas, the use of big data mining has quickly caught on, allowing insurance companies to quickly verify applicant's information through publicly available data and social media. Insurers are also utilizing social media to control targeted advertising.

Health Insurance companies have access to products such as Maya Intelligence (Accolade, Inc) which uses machine learning to detect the most relevant and cost-effective coverage for insureds and/or employers.

Trov is an example of an insurance technology platform which allows customers to buy mini policies for fleet transportation, electronic devices or renters insurance and allow coverage to be turned "on" or "off" by the customer.

Online "chatbots" are utilized to facilitate the quoting process and generate leads for agents.

### **B. Modeling**

Insurance companies have long used storm prediction models to monitor existing weather patterns. However, new studies such as the one spearheaded by Google, aim to predict flooding events and create early warning systems which can reduce deaths and economic damages by over a third. <https://www.livemint.com/companies/people/google-leveraging-machine-learning-to-predict-india-floods-1552193194482.html>

## **C. Underwriting**

Underwriting has always utilized predictive analytics. New tools for underwriting include the use of Geospatial imagery (drones) combined with machine learning tools to assess risk. IoT Sensors and “behavioral policy pricing” are becoming more common place – think of car sensors and fitness trackers. Progressive’s “safe driver” tool, for example, utilizes the information from the IoT sensors and puts it through underwriting software.

Some companies like Cape Analytics offer a service to help property insurers underwrite more accurately and cost-effectively using satellite-based machine vision which assesses information about the roof, property, treeline, pool, trampolines, etc. without sending someone to the property

AI is also used to spot anomalies and unknown correlations that would be impossible for the human eye to detect.

## **D. Claims**

Insurance Companies are introducing AI software into their legacy claims process and new companies like Lemonade are starting with an AI/behavioral-first approach.

Mobile apps allows drivers to assess damage in real-time at the scene of an accident using smartphone and images are processed by an AI model that creates an estimate. The software then compares the image to a database of similar images and allows the company to make smarter payout decisions.

AI can also make the claims process faster by using a chatbot, purportedly providing customers with faster payouts. These chatbots are designed to review the claim, verify policy details and pass it through a fraud detection algorithm before sending wire instructions to the bank to pay for the claim settlement.

## **III. Fraud Detection and Prevention**

When it comes to identifying fraudsters, insurers face a different fraud landscape with more players than most other businesses. Individuals commit insurance fraud in several ways, such as providing false information that gets them a lower premium. It is estimated that 10% of auto insurance policyholders falsely state that their vehicles are garaged at night. Applicants also lie about past claims history or place of residence. Unscrupulous agents embezzle premiums, and that is just at the underwriting stage. When we look at fraud in the claims process, companies must look at the claimants, third party providers and sometimes claims adjusters.

In healthcare, provider fraud includes false or exaggerated claims, medically unnecessary procedures, kickbacks for referrals and other schemes. Other types of provider fraud include overbilling for auto and home repairs. Auto shops and contractors may also charge for new parts and materials but use cheaper used items to make the repairs.

Organized crime rings have also been busted for scams against health insurers, federal crop insurance programs, homeowner insurers and commercial trucking insurers.

Faced with so many types of fraud from so many sources, insurers must look for better ways to screen applications, evaluate claims and identify bad actors.

### **A. Fraud Prevention**

AI can process relevant information and assess the risks around an insurance applicant more precisely and much faster than humans. Underwriters generally rely on information obtained from the applicant with little means of cost effectively verifying the validity and completeness of information.

Given sufficient data, Machine Learning can find patterns and flag potential fraud during the underwriting process. Relevant data stems from additional new online sources, including social media.

One technology company touts a “digital polygraph” to flag certain applicants. It uses AI to enhance risk scoring and automated underwriting algorithms to identify trends and suspicious patterns in behavior. For instance, if an applicant uses copy/paste to enter sensitive information, or delays answering questions they should readily know, or is repeatedly correcting entries, these can lead to an increased risk score.  
<https://www.formotiv.com/insurance-fraud-solutions/>

### **B. Fraud Detection**

The traditional methods of fraud detection involve fraud awareness by the adjuster or underwriter. Most companies conduct annual fraud awareness training and provide a set of ‘mandatory referrals to SIU’ when certain red flags are seen. Once potential fraud is identified, then the investigator conducts their own review to determine whether or not the red flag indicators detail potential fraud. These traditional methods include a human review for both detection and investigation.

Machine learning, or AI is used to detect red flags and recognize potential fraud patterns via several different methodologies, dependent upon the capabilities of the program, and the access it has to public and private data. For example :

- ❖ **KironMed (KironTech)** uses Machine learning to detect patterns of potential fraud or waste (overbilling).
- ❖ **SHIFT Technologies** uses a method of fraud scoring to detect potential suspect claims. Their data goes through a multitude of proprietary algorithms and then provides a score and the red flag indicators. Prior ISO claims history is not part of their data review, so they rely mostly on publicly available data, as well as the insurers data. They boast a 75% “hit rate”.

- ❖ **FRISS** is another proprietary program like SHIFT.
- ❖ **Claims Director** also uses fraud scoring and provides the red flag indicators , much like SHIFT, however their data includes ISO Claimsearch history. Therefore, they are in a better position to identify patterns and rings due to their accessibility of industry claims data.

Implementing Machine Learning within an organization requires substantial resources with training of both personnel and the data itself. Companies will need to work closely with their IT departments to ensure that the data provided is parsed in the best way possible to “connect” with the algorithms. Consistent review of the output and results is key in order to manipulate the data for the best output . The output should be consistent with the organization’s goals and objectives. The algorithms which work for one company, will not necessarily yield positive results with another. This massaging of the data needs to be a recurring function in order to adapt to the organization and the industry. An example is the creation of algorithms specific to Covid-19 schemes. Data points to support this may need to be added to the data feeds.

Once the AI program is in place, it will require constant supervision and analysis. Companies should not solely rely on the AI output . Human review to analyze the output is a must. AI and Machine Learning should be seen as a tool, not a solution. Although there are both supervised and unsupervised models, clearly models which employ data scientists who continuously supervise the results and output are preferred. Unsupervised models merely attach scoring to claims and leaves it up to the individual adjuster or investigator to determine the accuracy of the data.

Of note is that the implementation of Machine Learning within an organization will require a significant upfront investment, hundreds of thousands of dollars in most cases. In order to determine the impact and viability of the program and its efficiencies, it will need to be in place long term- for at least 2 years to see its full life cycle.

Companies who have implemented a successful AI tool to assist with the detection of fraud have seen an increase in the identification and investigation of common fraud problems. Some examples of this are :

- ❖ **Billing for services not provided**
  - ✓ AI scans records for documentation of services allegedly provided
- ❖ **“Upcharging” or “upcoding” for services**
  - ✓ AI can check typical treatments for similar injuries and detect anomalies
- ❖ **Kickbacks and referral relationships**
  - ✓ AI can analyze a mix of behavioral and transactional data to discover corruption
  - ✓ AI can provide data on connections/rings and this facilitates link analysis

#### **IV. Emerging Issues With the Use of Artificial Intelligence**

## **Ethical Considerations**

Artificial Intelligence has clear advantages in its rapid assimilation of data collection and processing of huge amounts of information. This speed and collation of personal information can bring to fruition predictive methodologies for insurance that quickly heighten profit margin. With the benefit quotient so high, ethical considerations become not only a necessity for employee and consumer protection and trust, but, indeed, must be a sacred cow for the current and future implementation and growth of AI systems. Proper consideration of ethical concerns and creation of safety measures will reduce litigation exposure for the improper use or dissemination of information and will reduce the possibility of other moral or ethical pitfalls.

## **Elimination of Jobs and Unintentional Bias**

Ethical questions regarding widespread use of AI abounds. Whole classes of jobs are being eliminated as AI systems become more ubiquitous. According to research from the World Economic Forum, 71% of total task-hours are currently completed by humans, compared to 29% that are done by machines. The World Economic Forum's 2018 study predicted that if current trends continue, the average will shift to 58% completed by humans and 42% by machines by the year 2022.

Thus, while advanced algorithms are increasingly being used in specific tasks like information and data processing, AI is also taking over a percentage of tasks that are still overwhelmingly human, like decision making, communicating, and coordinating.

AI vendors argue that machines can do it better, faster and with less errors. Without a doubt, AI aggregates and evaluates expansive amounts of data that cannot be analyzed by humans in the same fashion or time frame. But can machines completely eliminate the need for the human touch? Can machines take into account all external factors to determine if a particular action or course of action should be undertaken under the particularized facts of a given circumstance? Clearly the answer depends on the particular application being utilized.

At present, AI is utilized to make hiring recommendations, determine creditworthiness, determine risk factors and even predict whether a criminal will re-offend. Yet, AI systems, and how they actually make decisions, are a mystery to most people, with only their "creators" really understanding the intricacies of their inner workings. Couple this with an AI systems "unwitting" reinforcement of racial or gender bias gleaned from real world data, and you can have unfortunate outcomes.

For example, ProPublica analyzed a computer system created to help judges sentence criminals, that predicts the likelihood that criminals will re-offend. ProPublica's findings determined that the AI system was biased against blacks. <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

Amazon developed and briefly utilized a recruiting tool for identifying software engineers for hire. The system "learned" by combing through 10 years of resumes that had been previously

submitted to Amazon, which were predominantly male. As a result, the system favored male candidates. Once the bias was uncovered the system was abandoned. <https://www.businessinsider.com/amazon-built-ai-to-hire-people-discriminated-against-women-2018-10>

So, how do we protect from infecting pure computational processes and decision making with the implicit bias in the data inputted to create the systems? Training and educating computer scientists and analysts so that they understand how these things may occur is key. With these issues in mind, potential biases can be addressed at the programming stage and companies can monitor and correct any unintended consequences.

### **Data Collection and Ethical Uses of Data**

In today's society, data mining is everywhere and comes at us from all angles. It can be gathered by phone, by online methods, smart homes, social media or of course with personal interviews. Insurance carriers use these mining methods to gain a greater understanding to help guide their relationships in claims, underwriting and sales. You need a service, insurance, to purchase a car, to obtain a loan, to sign up for a new financial advisor, to use your favorite APP like Uber, or Postmates to deliver food. These all offer assistance and convenience to make our lives easier, but question is and remains: how is our information protected? What governs its sharing with other institutions? What if I don't want my information shared?

Let's say you need a sectional for your house and you do a little research on the Wayfair website or on their APP. Is it now our communal experience that whenever you open your smartphone or computer you get adds for sectionals on every platform you enter! There are algorithms at work for sure, but can you be sure that's all that is going on?

Just like Wayfair, Amazon and other retailers, insurance carriers use the information collected to deliver their products, advertise and have interchanges with clients and insureds.

The ultimate use of your information is guided by many federal privacy laws, such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes Oxley (Sox), Graham Leach Biley Act (GLBA). State laws may also apply. On January 1, 2020, California became the first state to enact comprehensive privacy legislation, the California Consumer Privacy Act (CCPA) that governs the collection, use and sale of personal information of California residents. Other notable legislation is the European Union's General Data Protection Regulation (GDPR) which requires companies to be able to explain decisions made by their algorithms.

Outside of privacy issues, there are no established laws specifically governing AI, However, a growing list of governments—the United States, the United Kingdom, Canada, China, Singapore, France, and New Zealand—have released AI strategies focusing on developing ethical frameworks, standards and policies. <https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd> While these efforts are still in initial phases, they signal the growing urgency inherent in ethical AI related issues.

In the end, any proposed AI policy should be based on certain foundational principles: Accountability, Fairness, Transparency, Diversity and Inclusivity, Privacy and Safety. The two

that tower over the rest are Fairness and Transparency because without these the others do not have the building blocks to stand on. Any data use or sale must be explained and be for the benefit of the insured. Fairness must be a hallmark of its use. Therefore, bias must be avoided at all costs because even slight bias within large scales of deployment can be detrimental to large numbers of people. So, in addition to built-in measures to cull potential bias, insurers should develop systems of redress, tracing, auditing, and appeals. AI, like all forms of information gathering, is hampered by the old adage “garbage in, garbage out”. The inclusion of diversity in your teams will hopefully help to capture even cultural differences and nuances so that the AI algorithms secure more fair, accurate and lawful outcomes.