THOMSON REUTERS

Westlaw®

Introduction to AI and IoT issues in product liability litigation

By Jonathan T. Barton, Esq., *Stanton Barton LLC**

FEBRUARY 20, 2019

"Robots cannot be sued."[1]

ARTIFICIAL INTELLIGENCE: WHAT'S NEW IS OLD

Product liability litigation has always focused on the functions and feature of the product. From the initial design to the warnings and instructions for use that accompany a product, every aspect has been scrutinized in the eyes of the law. Industrial machines have integrated programmable logic controllers ("PLC") with relays, interlocks and light sensors for decades.

In many machines the PLC decides what action to take based upon its programming and the input received from sensors. These "logic" systems operate on virtually every mechanized product available today from punch presses to the most advanced automobiles.

From basic input decisions such as keyless entry on an automobile and interlocking gates on a press to more complex decision making such as voice recognition, programmable logic systems have advanced to a level where the actions taken by these machines appear to mimic human comprehension as opposed to the designed, pre-programmed actions they are.

At some point in our history, within the last 20 years, the nomenclature used to describe this complex series of input driven "if-then" choices began to be described as artificial intelligence ("AI").

Merriam-Webster defines artificial intelligence as a "branch of computer science dealing with the simulation of intelligent behavior in computers" and "the capability of a machine to imitate intelligent human behavior."[2]

Notice the definition of artificial intelligence describes it as a mere "simulation" or way to "imitate" human reaction and not self-consciousness. This distinction is critical in the eyes of product liability litigation. We, as a society, are not yet at the stage where a machine can be said to have cognition, independent thought or free will.[3]

Even the most advanced computer learning algorithms are just that, programs telling the machine what and how to learn. These programming choices define and determine how the computer will learn and what action it will take based upon the input received.

Science fiction movies often depict a futuristic dystopian society where machines advance past their programming to some form of independent thought. It seems that in every movie where the machines gain consciousness their first decision is to eliminate mankind, except when they have been programmed to first do no harm.[4]

This nuance, the ability to place restrictions on a program and ultimately control what action or inaction is taken, inevitably brings us back to the realization that no matter what science fiction writers tell us, machines that incorporate artificial intelligence are just that — machines capable of programming and control.

Artificial intelligence is therefore a mere component part subject to the same scrutiny that exists within the traditional notions of product liability law.

Artificial intelligence is a mere component part subject to the same scrutiny that exists within the traditional notions of product liability law.

The change in nomenclature from a PLC to artificial intelligence has been driven by both marketing efforts and the need to distinguish the increased complexity and sophistication in the "intelligent" selection these machines are programmed to make.

This is distinguished from machine learning, which is using the programming and input data to create predictive models to mimic the human decision-making process.

Regardless, whether the program is described as a logic system, artificial intelligence or machine learning, it is just another component part of the product in the eyes of the law. Thus, it is just as susceptible to failure as a door latch or to problems caused by the inadequacies of an instruction or warning. The scrutiny artificial intelligence receives is no different than any other product liability claim.

As a result, the defense of such products follows the traditional model requiring an understanding the design aspects of the artificial intelligence, the input received, and how the machine

is programmed to react to such input. However, such information is not as readily observable as a fractured gear, a failed relay or an omission in an instruction manual.

The decision-making process or "intelligence" of such machines is wholly dependent upon the information or input received. Just as humans require information and historical experience to form a judgment and make a decision, so too do today's "intelligent" machines.

The design of the intelligence can create a technological challenge for attorneys defending such products just as the programming language of the PLC did decades ago. Programming changes, input storage and static memory in a product utilizing artificial intelligence create the same discovery hurdles litigators have grappled with throughout the history of product liability litigation.

Just as metallurgists are utilized to better understand defect claims of fatigue failure, so too are programmers used as consultants to review and interpret the data preserved. The only difference is the shear amount of data available within the ever-increasing complexities of programs utilizing artificial intelligence.

These challenges have become even more complex with the advent of the Internet of Things ("IoT"), connecting each of these artificially intelligent products to the Internet and each other.

THE INTERNET OF THINGS: THE BENEFITS AND PERILS OF CONNECTIVITY

The Internet of Things describes the connectivity and interaction of any device to each other and the Internet. In the consumer market, this includes everything from our smart phones and security systems to refrigerators and even lawn-mowers.

Virtually every aspect of modern life is enhanced in some way by this ubiquitous connectivity which, at its core, involves the receipt and transfer of information. Estimates range from 26 to 30 billion connected devices will be in use by 2020.[5] The economic impact of IoT ranges from $1.46 trillion to $3 trillion during the same time-frame.

As such, legal issues deriving from these connected products will play a role in the prosecution and defense of virtually every product liability matter involving machines going forward.

We are already seeing the dramatic impact these connected products can have in litigation scenarios across a wide range of cases. It is commonplace to utilize smartphone data to determine the location of individuals (or at least their phone) in automobile accident cases not to mention family or criminal law.

Personal consumer devices track virtually every aspect of an individual's life from where they are, how fast they are going, how many steps they take and even their heart rate. Consider the usefulness of such data when defending a personal injury case involving significant medical limitations.

While the testimony of the injured party and the retained physician may reflect a sedentary life, the individual's smart phone and fitness tracker paint a much different picture. Such data has become the DNA evidence of civil litigation. Jurors trust the output of the electronic devices and unlike DNA evidence, most, if not all, jurors have firsthand experience with such devices.

In the business environment, examples of how IoT has infiltrated the courtroom are equally as pervasive. Onboard GPS data has been used for decades to determine a truck driver's compliance with Department of Transportation regulations and to make employment decisions.

> Whether the program is described as a logic system, artificial intelligence or machine learning, it is just another component part of the product in the eyes of the law.

Now product manufacturers can remotely monitor a fleet of trucks and make recommendations in real time regarding fleet and individual vehicle productivity and maintenance.

Such capabilities can allow a business to reduce its overall fuel consumption, avoid maintenance interruptions and failures and improve efficiency and productivity across a number of metrics. Such capabilities are no longer in the in the exclusive control of the end user or purchaser of a product.

Manufacturers have the capability to monitor the information to create sales leads, provide specialized and focused services to end users and to improve their products.

Indeed, products utilizing IoT technology provide a wealth of information to those who know how to interrogate the code and analyze the output. While the utility of such information in the business setting is obvious, the question of who owns the data and who has a responsibility and/or duty to act on behalf of the end user is not. Therein lies the issue with connectivity.

From smart meters that monitor surges within the power grid to temperature sensors that can predict the overheating and failure of a component, these connected devices are in a place to provide more detailed and reliable data to litigators and the finder of fact.

Further, often these connected products utilize artificial intelligence to take action or make decisions based upon the input received.

For example, your "smart" thermostat monitors the temperature and humidity in your house and adjusts the

temperature according to the input it receives on your preferences and that of your family.

Your connected irrigation system may decide not to run if rain is in the forecast or if the ground is saturated.

In today's connected world you can control the hue of the lighting in your home at different times of the day and even dispense a treat to your pet from wherever you may be (even your living room).

In the industrial and manufacturing sector, these connections have much broader applications not only in supply chain and business to business interactions but with the end user. This direct connection between the product manufacturer and the end user throughout the life of a product has never existed in our history nor have the broader legal implications created as a result.

While maintaining a comfortable temperature in our home is important to us personally, maintaining the proper temperature in a data center for a banking institution is critical to their business. Overtemperature events may result in catastrophic failures, loss of data, down-time and business interruption.

When such events occur, who is responsible for the loss? Is it the end user who has a duty to maintain the products and monitor the temperature of the data center to avoid failure or the manufacturer who has access to the same or superior data?

Similarly, while an unsightly lawn may make you the pariah of your neighborhood, the failure of a commercial farm's irrigation system may cost millions and destroy an entire crop damaging the livelihood of the farmers who increasingly rely on such technology.

In such scenarios, litigation will ensue and questions will be raised on who had a duty to take action. These questions will turn on who had access to the information and what representations they made to the end user, if any.

IoT connectivity allows businesses to control a drill on an oil rig, monitor the location and status of a fleet of trucks, determine how much power is being used by a homeowner and inform the manufacturer of a product what service has been done and what service is required.

This connection allows manufacturers to monitor the use, functions and status of their products and sell additional services to its customers to improve productivity, enhance the functions of the products and avoid down time.

From automatic updates to the software to troubleshooting mechanical problems, the ability of the manufacturer to interrogate and perform diagnostic checks on a machine owned by an end user has blurred the once clear line of when the product leaves the care, custody and control of the manufacturer.

Indeed, the advent of this technology has fostered expectations that the sale of a product will include services to monitor and protect the end user from failures, expensive repairs and downtime.

These developments create new legal implications for how a manufacturer advertises and sells their products and services. Consider, for example, manufacturers advertising that through IoT connectivity they "possess the same or better data than the customer."

If true, what obligations exist on the manufacturer to act on the data? The answer may be none, however, what if the manufacturer claims to be able to "provide services based on data in real time" with access to "better data" than the end user?

If the manufacturer is in possession of "better" information showing an eminent failure and is in a possession to divert a shutdown, do they have a duty to act? In the absence of a service contract one might conclude that no duty exists.

The advent of this technology has fostered expectations that the sale of a product will include services to monitor and protect the end user from failures, expensive repairs and downtime.

However, with IoT integration many manufactures are touting their ability to predict failures and take proactive measures to reduce a customer's risk of down-time and business interruption.

These representations are akin to marketing on the relative safety of a product. No in-house counsel would ever allow their marketing department to claim that a product could "predict injuries, take proactive measures to prevent injuries or mitigate those injuries" for the simple reason that a manufacturer cannot insure against all unforeseeable act for the life of the product.

As IoT becomes more ubiquitous, manufacturers will need to consider the potential implications created by marketing a machine's ability to use predictive modeling and artificial intelligence to avoid business interruption.

These questions are just the beginning of the impact AI and IoT will have on products in the industrial and consumer markets. As product manufacturers increasingly act as intermediaries between the end users' data and the product, new duties could emerge.

Further, the old duties of ensuring that a product is free from manufacturing, design and warning defects at the time it leaves the care, custody and control of the manufacturer may be extended because of this connectivity.

The ability manufacturers now possess to gather and analyze a customer's critical information from their product post-sale and take action to avoid or mitigate loss will inevitably lead to questions concerning what, if any, duty to act exists. While the robots cannot be sued, their manufacturers can.

NOTES

[1] *United States v. Athlone Indus., Inc.*, 746 F.2d 977, 979 (3d Cir. 1984).

[2] https://bit.ly/2x8Llve.

[3] True artificial intelligence or decision making wholly independent of its creator runs afoul of the current notions of causation. *See e.g. Palsgraf v. Long Island R. Co.*, 248 N.Y. 339 (N.Y. 1928) In the context of our current artificial intelligence capability, it is the machine's design, or more precisely, that of its programming that informs the action. That said, if artificial intelligence advances past the programming into an unknown and truly independent act, how then can we blame the creator for the independent acts caused by this artificial intelligence? Commentators have suggested the law bend the notion of causation allowing for variations of responsibility known as the "Turing Registry." Curtis E.A. Karnow, *Liability for Distributed Artificial Intelligences,* 11 Berkeley Tech. L.J. 147, 175 (1996). While such proposals provide a solution to a specific problem they also create the inevitable slippery slope of liability and causation. If we allow the creator to be even partially responsible for the independent acts of the product, then what is to stop us from imputing liability to third parties for the poor decisions made by natural intelligence because of bad input (i.e. parents, teachers, bullies etc.).

[4] Compare The Terminator (1984) with I, Robot (2004) and Bicentennial Man (1999) wherein the latter use the application of The Three Laws created by science fiction author Isaac Asimov as a pre-programmed design feature to prevent harm. The Three Laws state that a robot may not injure a human being or, through inaction, allow a human being to come to harm. Further, a robot must obey the orders given [to] it by human beings except where such orders would conflict with the First Law and that a robot must protect its own existence as long as such protection does not conflict with the First or Second Laws. Asimov, Isaac, *Runaround* (1950).

[5] MacGillivray, Carrie, Worldwide Internet of Things Forecast Update, 2015-2019, International Data Corporation (IDC), February 2016.

This article first appeared in the February 20, 2019, edition of Westlaw Journal Medical Devices.

ABOUT THE AUTHOR

Jonathan T. Barton is a founding member of **Stanton Barton LLC** in St. Louis. He is a member of the firm's products liability practice group and is active in its general litigation and business litigation practice. He has experience in defending against products liability cases involving a wide array of industrial machinery, motorized vehicles, electrical components and consumer goods. He regularly defends manufacturers in catastrophic cases involving fire science. He also is a member of the Product Liability Committee of the International Association of Defense Counsel. He can be reached at jbarton@stantonbarton.com. This article was first published in the October 2018 issue of the IADC Product Liability Newsletter. Republished with permission.