WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

PRODUCT LIABILITY
Attorney Article

The Impact of the Smart Home Revolution on Product Liability and Fire Cause Determinations

September 12, 2016

H. Michael O'Brien
Partner, White Plains
914.872.7234
michael.obrien@wilsonelser.com

1133 Westchester Avenue
White Plains, NY 10604

For more information about Wilson Elser's Product Liability practice visit our website.

The concept of the Internet of Things (IoT) has existed for more than 15 years. Technology pioneer Kevin Ashton is widely credited with coining the term in 1999 to describe the connection of physical objects to the internet via sensors. The IoT has become a reality with 6.4 billion devices connected to the internet and on average more than 5 million new devices connecting each day. Forecasts indicate that by the end of the decade more than 25 billion devices will be connected to the internet. The exponential growth of the IoT has been described as the Fourth Industrial Revolution, characterized by a fusion of technologies that is blurring the lines between the physical, digital and biological spheres. What makes the IoT dynamic is the ability to control products, machines and systems over the internet.

Within the broad expanse of industry sectors where internet adaptability is advancing, the connected or "smart home" is at the forefront. It embraces all manner of previously dumb household products, building systems and appliances that now can be connected to the internet to perform new functions and communicate with data centers or other smart devices. Among the appliances, consumer electronics and home systems that can connect with and be controlled over the internet are home security systems, garage doors, heating and air conditioning systems, refrigerators, ovens, ranges, washers and dryers, televisions, home entertainment, lighting, outlets and switches.

Continued

Gartner, Inc. has predicted smart home growth to go from 339 million applications in 2016 to more than a billion by 2018. *Business Insider Intelligence* has estimated that by 2019 companies will ship 1.9 billion connected home devices with estimated revenue of $490 billion. The driving forces behind this growth include the reduction in the cost of sensors, expanding internet connectivity, the desire for improved efficiencies and energy cost savings. Also, there is the drive to monetize big data generated from the use of these products where information on consumer use patterns and other valuable insights can be gleaned and used by businesses to generate market share and revenue and stave off the threat of new competitors.

THE INSURANCE INDUSTRY AND THE IoT

Insurance companies are embracing the IoT to drive customer service, provide user-based coverage options, track driving and user behaviors, and crack down on fraud. The insurance industry also is embracing the IoT because of the threat posed by technology giants that already have a significant advantage over insurers because of their daily interactions with consumers over the internet. Such interactions allow the technology companies to monetize data they collect in ways that could not be imagined a decade ago.

In the smart home arena, a number of property insurers have partnered with companies such as providers of home security services and smart home technologies to promote the use of smart devices and products in the home. Among the benefits touted are energy management, fire and water alerts, and home security. On a more granular level, these benefits include regulating home temperature; automating interior and exterior lights; using motion sensors to turn off lights when no one is present in a room; remotely turning off TVs and small appliances that were accidentally left on; remotely accessing temperature sensors; sending alerts when water is detected; locking or unlocking doors remotely; receiving notifications from your smart device; and detecting glass and window breakage. However, each of these features adds complexity to the functionality of the product or system and, like any product, can fail in ways not intended or anticipated. A device that can turn off a smart product also can turn it on. A device that can regulate temperatures can cause temperatures to reach dangerous levels.

LIABILITY AND SECURITY RISKS

With all the apparent benefits of smart home technology come potential risks. Dumb products made smart by connecting to the internet present a new layer of complexity when a failure occurs. The Nest thermostat, which can be controlled by a smart phone or tablet, experienced a software malfunction in January 2016 that caused the devices to lose power and drain their batteries, which could not be recharged by the software programming. Inoperable thermostats led to complaints of homes being left cold and the potential for water pipes to burst. Other reported smart home product failures include internet phone service and internet security system failures.

It is a given that anything connected to the internet is vulnerable to a cyber-attack. Until recently, the threat of cyber-attacks has been limited largely to the theft and misappropriation of data. However, with smart home applications, a cyber-attack on an IoT-connected product or system has the risk of causing property damage, bodily injury or death. In an August 2016 interview, Elliot Kaye, Chairman of the U.S. Consumer Product Safety Commission, reported that the CPSC was assessing the risks to consumers posed by emerging technologies, including the IoT, and identified concerns with the potential safety of devices that can be hacked or where a software update to fix a problem is not installed.

Continued

The Federal Bureau of Investigation and other federal agencies, including the Federal Trade Commission and Department of Homeland Security, also have identified IoT-connected devices as being vulnerable to cyber-attacks that can lead to property damage, bodily injury or death.

IMAGINED VERSUS REAL THREATS

One of the first demonstrations of a successful cyber-attack was the Aurora Vulnerability test conducted in 2007 at the Idaho National Laboratory. A computer was programmed to cause a diesel generator's circuit breakers to open and close out of sync, eventually leading to an explosion. A video of this demonstration provided by the Department of Homeland Security was released by CNN in 2007 and can be viewed on YouTube.

A number of other documented cyber-attacks have caused property damage dating back to the Stuxnet attack on the Iranian nuclear energy facility by the United States and Israel in 2010. In 2014, a German steel mill was attacked

and a blast furnace was destroyed. In 2015, Fiat Chrysler recalled 1.4 million Jeep Grand Cherokees because it was demonstrated by white hat (ethical) hacktivists that the infotainment system of the vehicle was vulnerable to a remote cyber-attack that could cede control of critical operator and safety controls to remote hackers. In December 2015, the power grid in western Ukraine was attacked and shut down for several hours, reportedly by a Russian state-sponsored cyber-attack.

INVESTIGATING FIRES INVOLVING IOT SMART DEVICES

When fires occur in insured structures, the property insurer will investigate to adjust the first-party loss suffered by the policyholder and then look to address the potential for a recovery of monetary damages by subrogation against a responsible third party, such as a product manufacturer, if the product is thought to have played a role is causing the fire. This undertaking requires that a qualified fire investigator − often a Certified Fire Investigator (CFI) or Certified Fire and Explosion Investigator (CFEI) − and forensic engineer conduct an investigation in an effort to establish the area of origin of the fire and the possible cause of the fire.

NFPA 921

One of the primary reference guides used to aid with the investigation of fires is the National Fire Protection Association's NFPA 921 Guide for Fire and Explosion Investigations. However, neither the current edition (2014) nor the 2017 edition scheduled to be published shortly addresses "smart" products and the IoT where software malfunctions with previously dumb products have the potential to cause a fire. Another edition will not be published until 2020.

Continued

Chapter 3: Basic Methodology of NFPA 921 requires use of the "scientific method" to conduct an origin and cause determination by first recognizing the need and then defining the problem. However, when a technological revolution is taking place that is not yet recognized or understood by those charged with the investigation, it raises a question as to the underlying thoroughness and reliability of the investigation process if potential causes are overlooked or misunderstood. Another question arises as to whether current fire investigators and forensic engineers are equipped by education, training and experience to handle the complexity of fire investigations where internet-connected products with advanced software and sensors are deployed.

In addition to software or sensor failures, NFPA 921 will eventually have to address cyber-based attacks on internet-connected products as a potential cause of fires. An arson or incendiary fire is addressed in Chapter 24 of NFPA 921, where an incendiary fire is defined as "a fire deliberately set with the intent to cause the fire to occur in an area the fire should not be." Despite recognition by federal agencies that IoT devices can be hacked and cause physical damage, there is no discussion in NFPA 921 about internet-connected devices having the capacity to be used to deliberately start fires. It is worth noting that while Chapter 24 identifies a number of motives behind incendiary fires − including vandalism, willful and malicious mischief, excitement, thrill seeking, attention seeking, recognition, extremism and terrorism − these same motives can be said to apply to individuals who commit cyber-attacks.

While internet-connected products, appliances and systems are not directly addressed in NFPA 921, there is some recognition of the importance of data and information that these devices and systems hold that might be relevant to a fire investigation. However, these sections are limited to collecting data that is stored on hard drives, not in the cloud or on servers or other devices such as smart phones, tablets and routers.

For instance, *Chapter 18: Origin Determinations* makes reference in various sections to specific appliances and systems that might contain retrievable data.

18.3.3.11 Fire Protection Systems. …If the system was monitored, records should be obtained from the monitoring service. In some instances, information can be downloaded from the central panel to indicate alarm and trouble signal locations and times. … A qualified technician should be employed for downloading the data as substantial permanent loss of data can occur if this is done incorrectly….

18.3.3.8 HVAC Systems. …Some systems are equipped with manual or automatic dampers designed to control fire spread, smoke movement, or airflow. Where these devices are present, their specific location and condition should be noted and any activation records should be obtained. The location and setting of any thermostats, switches, or controls for the HVAC system should be identified and documented.

18.3.3.13 Security Cameras. Security cameras that monitor buildings … may be very useful, particularly for "hard" times. Events before or during the fire including, in some cases, the actual ignition and development of the fire may have been recorded. The video recorder may be found in a secure area or a remote location. It should be recovered and reviewed even if damaged.

*18.3.3.14 Intrusion Alarm System*s. An intrusion system may activate during a fire due to heat, smoke movement, the destruction of wiring, or loss of power. A monitored intrusion system may send a trouble signal to the monitoring station if a transmission line is compromised or power is lost. As with fire alarm systems, attempts should

Continued

be made to recover the alarm panel history before the alarm system is reset. This frequently requires special expertise. Some alarm systems may record the identity of persons entering or leaving the building.

However, none of the subsections referenced recognize that these products and systems if connected to the internet can potentially be the cause of a fire due to software or sensor failure or that they may be vulnerable to cyber-attacks by hackers who could gain control of the products and systems in order to cause damage. In fact, a search engine called Shodan has servers located around the world that crawl the internet 24/7 to provide the latest internet intelligence. Shodan is used to find IoT-connected devices around the world, including "cars, fetal heart monitors, water treatment facilities, power plant controls, traffic lights and glucose meters." (*See*, "The Terrifying Search Engine That Finds Internet-Connected Cameras, Traffic Lights, Medical Devices, Baby Monitors and Power Plants," *Forbes*, September 23, 2013) Shodan recently launched a new section that lets users browse webcams that are vulnerable because they use the Real Time Streaming Protocol to share video but have no password authentication in place. The image feed is available to paid Shodan members who can search using the site's filter port.

On a more positive note, NFPA 921 *does* recognize the need to call in new expertise when the investigator finds that the data to be analyzed is beyond his expertise.

18.4 Analyze the Data. The scientific method requires that all data collected that bears upon the origin be analyzed. This is an essential step that must take place before the formation of any hypotheses. The identification, gathering, and cataloging of data does not equate to data analysis. Analysis of the data is based on knowledge, training, experience, and expertise of the individual doing the analysis. *If the investigator lacks the knowledge to properly attribute meaning to a piece of data, then assistance should be sought from someone with the necessary knowledge*. Understanding the meaning of the data will enable the investigator to form hypotheses based on the evidence, rather than on speculation or subjective belief.

Chapter 19: Fire Cause Determination has language that is very similar to the language in the section above addressing the analysis of the data.

Section 19.4, like *18.4*, provides: Analysis of the data is based on knowledge, training, experience, and expertise of the individual doing the analysis. *If the investigator lacks the knowledge to properly attribute a meaning to a piece of data, then assistance should be sought from someone with the necessary knowledge*. Understanding the meaning of the data will enable the investigator to form hypotheses based on the evidence, rather than on speculation or subjective belief.

In the context of the smart home, other chapters that will eventually need to address the IoT are *Chapter 26: Appliances and Chapter 26.4.2: The Use and Design of the Appliance*.

LACK OF STANDARDS

Another area that will complicate the investigation process for the immediate and near future is the lack of safety standards. Most common household products that are powered by electricity, batteries or carbon fuels have the potential to fail in various modes of operation, which can lead to fires. This recognition has led to the development of standards through safety organizations such as Underwriters Laboratories (UL) working with industry, government and consumer safety groups. These efforts are used in part to address potential product failures through the development of consensus safety standards that incorporate designs to mitigate against failures. But when a dumb product is connected to the internet and is given smart applications, the smart features may have the potential to cause the failure of the product. How then does the governing product safety standard address this new technology?

At present, none of the existing UL standards for home appliances, consumer electronics or home-building systems have any safety requirements to address software applications and connectivity to the internet.

Continued

UL 2900-1

UL, however, has taken the first step to begin to examine this risk. In April 2016, it launched its Cybersecurity Assurance Program (CAP) with the introduction of UL 2900. UL 2900 is not a standard; rather, it is an outline for the eventual development of a standard. There are three outlines in all. The first is UL 2900-1 Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements. The other two apply to the health care industry and industrial control systems.

According to Underwriters Laboratories, UL 2900-1 "provides a minimum set of requirements that developers of network-connectable products can pursue to establish a baseline of protection against vulnerabilities and software weaknesses, along with a minimum set of security risks controls and documentation to consider relative to their existing overall product risk assessments."

UL touts 2900 as "part of a series of standards to offer testable cybersecurity criteria for network-connectable products and systems to assess software vulnerabilities and weaknesses and minimize exploitation, address malware, review security controls and increase security awareness."

UL acknowledges that "… interoperability, security and data privacy become critical when connecting devices via public networks. … security attacks and breaches on connected cars and electric goods have been demonstrated … and … can be life threatening."

UL's initial efforts seemed directed toward software vendors, start-ups, manufacturers deploying IoT products and buyers of these products "looking for trusted support in assessing security risks while they continue to focus on product innovation to help build safer, more secure products, as well as for purchasers of products who want to mitigate risks by sourcing products validated by a trusted third party."

The scope of the outline "applies to network-connectable products that shall be evaluated and tested for vulnerabilities, software weaknesses and malware."

The outline sets out areas to be addressed, but does not provide any guidance on how this is to be accomplished. Areas to be addressed include:

a. Requirements regarding the vendor's risk management process for its product

b. Methods by which a product shall be evaluated and tested for the presence of vulnerabilities, software weaknesses and malware

c. Requirements regarding the presence of security risk controls in the architecture and design of a product.

Notably the "outline does not contain requirements regarding functional testing of a product" and therefore "contains no requirements to verify that the product functions as designed." Nor does the outline "contain requirements regarding the hardware contained in a product."

Thus far, UL's effort is largely conceptual as there is no standard for products that are governed by a UL standard that addresses their software, sensor and internet connectivity applications. The actual criteria of practices and procedures contained in the outline is generalized and more of a "what to do" rather than a "how to" set of requirements. Moreover, there are no existing safety standards for anything that is considered an IoT product. While various safety organizations and stakeholders are working on developing standards that will address issues, including security and safety, for the foreseeable future technology is again outpacing the regulatory efforts to keep up with the new technological advancements.

Continued

SECURITY VULNERABILITIES

Going forward, the investigation of a fire that may involve an IoT product will need to take into account the vulnerability of the device to hacking. Lack of encryption and use of default passwords from the manufacturer provide easy pathways for hackers to gain access to smart devices. In 2016, a research team at the University of Michigan published a study addressing vulnerabilities with Samsung's SmartThings platform. The researchers were able to (1) exploit the SmartApp to program backdoor pin-codes to a connected locked door and (2) eavesdrop on a smart lock when it was being programmed, disabling the vacation mode and causing a fake fire alarm.

In February 2016, the Federal Trade Commission announced a settlement with ASUS, a Taiwanese multinational computer hardware and electronics company, where it agreed that its routers used in consumer home networks were vulnerable to security breaches, placing consumers' networks at risk for cyber breaches. While the emphasis was on privacy and data vulnerabilities, the insecurity of the router could lead to products connected to the router falling under the control of a hacker.

In August 2016, researchers at the DEF CON 24 security conference demonstrated the vulnerabilities of smart lock padlocks and door locks. Others demonstrated how the vulnerabilities of smart thermostats to hacking can lead to denial of service.

INTEROPERABILITY AND INTERCONNECTIVITY ISSUES

Interconnectivity and interoperability are terms often misunderstood and occasionally used interchangeably. Interconnectivity addresses the ability to connect a device to the internet and to operate and communicate with it, often as part of a stand-alone ecosystem.

Interoperability deals with the ability to connect a series of distinct connected devices or ecosystems so that they can communicate and operate with each other. One useful definition posited in an article by Stephanie Lynn Sharron and Nikita A. Tuckett is "the ability of objects or devices, whether they be sensors, computers or other everyday things, to connect with each other and communicate data in a form and format that can be understood and processed by other persons or entities and is agnostic as to the hardware or software on which the data is to be further processed and stored."

Interoperability is one of the foundational challenges facing the growth of the IoT as each competitor is looking to create its own operating system to manage and control its products.

In the smart home arena the issue of interoperability of various platforms of IoT devices is an obstacle to harmonization and a potential area of vulnerability. All major players have made investments in their own proprietary platforms. Samsung has SmartThings, Google has Thread, Apple has Home Kit and Amazon has Echo. Different software platforms will each have different security issues in addition to the expected software glitches that have already been demonstrated in recent years.

As new players make their push into the smart home ecosystem, it is a given that smart appliances will be in homes, each potentially operating independently on their own proprietary software, which in turn will be managed by a smart phone or tablet from yet another company with its own software. Thus, a washer and dryer made by one company will be in a home where there is a smart thermostat made by a second company and a smart security system made by a third. In turn, all of these devices may be managed by a smart phone or tablet made by yet another company. The smart phone/tablet may have its own propriety software controlling the smart devises or it may use software supplied by an outside vendor. Thus, the lack of interoperability among various IoT platforms will likely add more complexity to fire investigations.

The complexity of the supply chain of smart home technology will likely make it harder to establish liability when a failure due to either a software malfunction or a cyber-attack causes a fire. The legal definition of what is a "product" also is likely to complicate the effort to establish fault and assign liability to a responsible third party. Software is usually viewed by the courts as a service rather than a product, which may curtail what theories of liability can be employed to make a legal claim against a smart device.

Continued

In addition, the design of the application, or app, that runs the programs for the smart things requires two different sets of software. First, there is the communication-transmission software that exists with the smart product, and then there is the communication-receiving software that resides on the smart phone or tablet. The software may be proprietary to a manufacturer of the smart product or it may be sourced from a software vendor. Likewise, the software on the cell phone or tablet may be propriety or sourced.

Poor security protections in the form of easily guessed default passwords or those that can be breached via "brute force" attacks present an avenue of security risk. Encryption is advocated as an additional measure of security to reduce the likelihood of a cyber-attack that succeeds in gaining access to and control of a smart product or ecosystem.

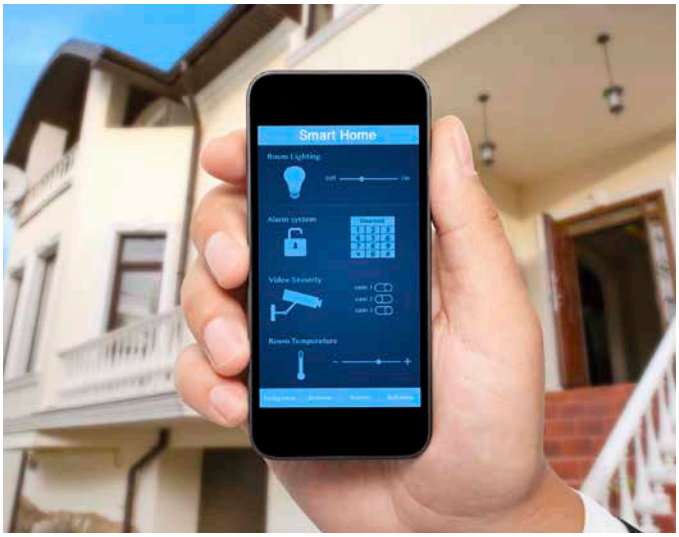
E-DISCOVERY AND PRIVACY ISSUES

The complexity of smart devices in the home is further compounded by the wide range of different programming systems being deployed by IoT manufacturers. There are, for instance, issues with interoperability − the ability of a system or a product to work with other systems or products without special effort on the part of the customer.

As noted, the design of a smart app involves two sets of software: the software that enables communication by the IoT product and the receiving software in the cell phone or tablet from which the consumer controls the product. Multiple parties can be involved with the development of the software for both the IoT product and the control. This further complicates the identification of potentially responsible third parties and the determination of fault.

How does an injured party establish that software malfunctioned and caused the product to fail? What kind of information obtained through lab examinations or in pre-trial discovery will need to be examined to make this work? IoT devices already have been examined in the context of personal injury lawsuits. A Canadian lawyer has used the data from his client's Fitbit band in an effort to establish her pre- and post-accident levels of physical activity. The NFL undertook steps to obtain data during the investigation of Deflategate and attempted to obtain New England Patriot quarterback Tom Brady's cell phone to examine his emails and text messages.

The question of privacy versus the reasonable needs of litigants is likely to be a major issue in civil litigation when IoT products are the subject of a lawsuit. The issue of data ownership also is likely to add complexity to litigation in which a smart product is at the center of a claim. Is the data owned by the manufacturer, the wireless service provider or the consumer?



It may be ironic that the proliferation of smart home devices is being driven by the very same property insurers who will seek recovery for fire losses against an IoT device when it is identified as a viable subrogation target. In the context of privacy and ownership of data, this may create a conflict issue. One insurer as part of its promotion of smart products has privacy policies that state the insurer may use customer information to process claims, among other things. But if an insurance company has promoted the use of smart technology for its insureds and has collected information to create efficiencies and improvements or to monetize the information, should the insurer then have access to discoverable information that may be relevant to a subrogation claim it may make against a potentially responsible third party?

Continued

CLOSING THOUGHTS

The potential for an internet-connected product to experience a software or sensor malfunction that can cause a fire is something that will have to be addressed by manufacturers, insurers and other stakeholders in the IoT marketplace. In addition, because IoT products are vulnerable to cyber-attacks, manufacturers, insurers and other stakeholders will have to address the deliberate actions of hackers that can induce a failure leading to damage. Hence, when the failure of a smart product leads to a fire, the challenge of how the smart home application should be evaluated and examined as a potential cause becomes a more complex undertaking than the failure of a similar but dumb product.

Lawyers who defend manufacturers in product liability fire losses will likely be the first to challenge expert findings from a fire scene investigation and laboratory analysis of evidence and artifacts collected post-fire if IoT-connected products found at the scene are not addressed in a way that takes into account the new complexities and vulnerabilities. In particular, the ability to ”rule out” an IoT product rather than point to it as a cause may be more problematic if the investigator and experts retained to conduct the cause and origin investigation fundamentally do not understand the complexity of the smart products − or until the standards catch up with the technology.