

Hey Google! **WHERE DID THE FIRE START?**

Nicholas Mahoney, P.E., CFEI, CVFI S-E-A

Hey Google! Where did the fire start? It sounds like a simple question, but it's not that easy! Siri, Alexa or Google Home devices can play music, relay the weather or tell you the latest sports scores, but what if these devices could also help with fire investigations if an accident strikes your home? It turns out they can, and it's more than a simple question.

Smart home devices such as smart speakers, thermostats and security cameras have increased in prevalence in recent

years. Some insurance and utility companies have even started offering incentives for smart home device installations. In some cases, these companies partner with device manufacturers to provide packages, including thermostats, cameras and security sensors. The benefit for homeowners is the ability to better manage power consumption or manage threats like burglary, fire or water damage. For insurance companies, the benefit is a potentially smaller

claim value when the insured is notified early or possibly remotely about these threats, thereby reducing damage and the costs for repairs.

Broadly speaking, a smart home device is any electronic device in your home, usually with wireless capability, that can act autonomously or interactively. Common examples are thermostats such as the Google Nest, doorbell/security cameras such as the Amazon Ring or smart speakers like the

Amazon Echo. The market has also grown to include larger products such as ranges, microwave ovens and refrigerators. Smart home devices are typically accessible over the home's Wi-Fi network or a user's mobile phone via Bluetooth. Even for products without a wireless connection, there is now the possibility for that device to be controlled remotely. Smart plugs and smart switches can turn any outlet into a piece of smart home technology. Aside from wireless connectivity, smart devices almost always include one or more electronic sensors, a processor and on-board or cloud-based data storage.

Examples of electronic sensors in smart home devices include cameras, microphones, temperature sensors and motion sensors. Each of these types of sensors can provide useful information for fire investigators. A typical security camera may pair a motion sensor with a camera to not only detect intruders but also detect the motion of flames or smoke and begin video recording. Many devices, including thermostats, can monitor the temperature in a room and track a fire's progression through a structure. Smart home speakers can record fire-related data as well. A feature added to Amazon's smart speakers includes the ability to monitor and record smoke alarm activation sounds while the homeowner is away. When the feature is enabled, a notification will be sent to the owner's mobile device in the event a fire is detected. These are just a subset of potentially useful sensor data, but none of these sensors can be used unless the data is processed and stored.

Processors are the brains of a smart home device, but the most intensive processing, especially for speech and video data, is often done at a remote data center. For example, only the word "Alexa" is deciphered by your speaker if you ask, "Alexa, what is the weather forecast today?" The entire question is then processed and stored in the cloud (at a data center).

Data retention is one critical differentiating factor among manufacturers. Depending on the device and manufacturer, cloud-based data could be deleted automatically, after ten days, as in the case of the Nest thermostat, or retained indefinitely as in the case of Amazon's Alexa devices. With such a variation in data retention, preservation of evidence for smart device data presents emerging legal issues. In some cases, it may warrant sending a preservation of evidence letter to the device manufacturer. This discrepancy in retention policies compounds the need for timely fire investigation by a qualified fire investigator.

An increase in ownership of smart

home devices has led police and fire departments to attempt to utilize their data. Some manufacturers allow consumers to opt-in, providing public agencies access to data like camera footage to aid with an investigation. Even without direct access to data, public agencies have seen benefit in these tools. Recently, in several cases in Virginia and Washington, smart smoke detectors were attributed with reducing fire service response time. In these cases, the homeowners were away when they received alerts on their mobile phones indicating smoke was detected. The homeowners were able to call 911, and the fire departments extinguished the fires before there was extensive damage to the homes. A quick response from the fire service can limit property damage, but it can also save more evidence of the fire's origin and cause. The evidentiary benefits of smart home devices extend further when considering the digital data available and its potential use in fire investigations. To utilize the data from smart home devices, a fire investigator must understand smart home device construction, how these devices store data and how exactly that data can assist in fire origin and cause investigation.

The use of electronic data in fire investigation is not a new idea. Witness information and/or electronic data is one of the three recognized sources of information for origin determination listed in the 2021 edition of NFPA 921, Guide for Fire and Explosion Investigations. As part of investigating a fire, using the scientific method as defined in NFPA 921, a fire investigator must collect data, analyze the data, develop hypotheses and test those hypotheses. The most fundamental part of the fire investigator's job comes in the development and testing of hypotheses of the origin and cause of a fire. Smart home technology simply provides another source of data that a fire investigator can use to develop origin and cause hypotheses.

Timeline development is one area where smart device data can help develop a hypothesis. A timeline using such data could incorporate events identified in video footage, but other data from smart devices can also be utilized. Many smart home systems keep a log of each device's status along with a time stamp, indicating when a device connected to Wi-Fi or when communication was lost. When fire attacks such a device causing it to lose power, the event is time stamped and logged. Now, consider a home - with several such devices that was completely burned. Rather than processing the entire fire scene, an investigator can reduce the area of interest by examining

data from the smart device log, identifying which device lost power first.

Smart home technology may also complicate a fire investigation. Smart home devices are connected to an owner's home network and often connected to the internet such that they are accessible via the owner's mobile phone or tablet. This connectivity means that fire investigators must consider the possibility of a remotely initiated fire. With appliances such as microwave ovens and ranges being given smart capabilities, the possibility exists for ill-intentioned users or hackers to remotely start a fire. For a fire investigator, these scenarios represent more potential hypotheses for fire origin and cause, but the evidence to support these hypotheses may not always be easy to obtain.

A question often raised in relation to digital data is one of ownership. If a consumer buys a smart device, who owns the data recorded on the device? In the European Union, regulators have attempted to address the issue head on with the General Data Protection Regulation (GDPR), which, among other things, attempts to require that individuals own their data and can access or delete the data upon request. Recent legislation in the United States has been more focused on security. So, as of the writing of this article, the privacy policy for a smart home product may include provisions that the manufacturer owns and may retain the data stored in its data centers. In that case, a subpoena may be required to gain access to the data.

Many common products in the home can now be considered smart home devices. Data from these devices can be potentially useful for fire origin and cause determination; however, fire investigators must know what to look for, what questions to ask, and when to enlist the services of a technical expert such as an electrical engineer. From there, time is of the essence when it comes to gathering data. While smart device data is unlikely to be the sole evidence used in determining a fire's origin and cause, in some cases, it may be the critical piece of data required.



Nick Mahoney, P.E., CFEI, CVFI is an electrical engineer in SE-A's Atlanta, Georgia, office. His responsibilities include the investigation of electrical faults and malfunctions, particularly those suspected of causing a fire, equipment damage, or personal injury due to shock or electrocution.