



Hi, I'm Listening

The Rapidly Increasing Use of Personal Assistants and Smart Products Provides Opportunities in Claims and Litigation

BY PETER A. LYNCH

Personal assistant data products, such as Amazon's Echo and Dot, Google Home, and others, are being aggressively marketed today. Amazon reports that it has sold five million Echos since its introduction two years ago. Google Home recently was introduced to compete with Amazon Echo in the personal assistant marketplace for use in homes and businesses.

With both of these products, a user gives a voice command to the product's operating system that then is processed and responded to. This type of technology was the centerpiece of the blockbuster 1968 movie *2001: A Space Odyssey*, in which Hal, an artificial intelligence computer, worked with astronauts to control most of their spacecraft's operations, including talking to them. Ultimately, and unfortunately, Hal had to be disconnected because he began killing crew members.

Today's personal assistant products allow users to get answers to queries that used to be done through a manual internet search on a computer or through smartphone assistants like Siri, Google Now, or Cortana. Personal assistant devices now are being used in homes and businesses to control smart products such as refrigerators, stoves, heating and air conditioning, nanny cams, and smoke detectors. All of these products store information that was previously not available or recoverable. Moreover, most products involve the use of apps where information is transmitted to the cloud onto a company's proprietary servers. It is then stored, and those companies can use it internally for targeted marketing, or they can sell the information.

With each technological advance, more and more data is collected by these products, which are sold by an array of disparate private businesses. With each advance, there is the potential to recover data from the product itself or from servers about what was happening at or near the device at the time of a loss. This article examines the most common personal assistant devices, touches on smart products controlled by them and what may be recoverable for use in potential litigation from these products, and counsels caution when buying them for your own home or business without considering the impact of what they monitor. These products can be seen as

positive developments for making life easier and safer when used appropriately and when data is protected.

PERSONAL/VOICE ASSISTANTS

The Echo, sold by Amazon, currently is the best-selling personal assistant device. It is a Wi-Fi connected tower speaker that acts as your in-home personal assistant by invoking Alexa, its operating system.

How is it set up? Place the device where desired and at least eight inches from walls or windows. Simply download the Alexa app and sign in. Set up the device on your phone or tablet to include managing alarms and more with third-party content developed for Echo. Turn Echo on by plugging the power adapter into an outlet. When the light turns orange, Echo will greet you. Follow the app instructions to connect Echo to a Wi-Fi network. Start talking to Alexa using the default wake word or choose your own. Echo has seven microphones with noise cancellation to include far-field voice recognition. It is always on and listening unless a button is physically pushed turning it off.

Why is Echo so popular? It was first to market, giving it a competitive advantage that Google Home is seeking to overcome. Appropriately set up, Echo can provide information or news, turn off lights, turn on music, and control smart systems and appliances.

Echo updates to the cloud and learns speech patterns, personal preferences, and your vocabulary. Companies that have partnered with Echo include Uber, Fitbit, Netamo (heating system), and Honeywell systems. Amazon has recently released Amazon Dot, a compact version of Echo, that can be placed throughout an area to increase access to the personal assistant services.

Google Home. Google Home is another voice-activated speaker that works with Google Assistant. Again, it receives voice commands to answer questions; gets information such as weather, traffic, and news; and conducts operations such as those done by the Echo. It can connect to smart devices like Chromecast, Nest, and Philips Hue that can control thermostats, light controls, smart plugs and switches, etc.

Samsung Otto (Prototype).

Amazon Echo and Google Home grab the most attention and sales in the personal assistant device category. However, Samsung has a prototype virtual assistant, called Otto, which is similar to the Amazon Echo but with a high-definition camera. Otto will be able to stream video live to your phone or computer. Its head turns, swivels, and pivots to look around the room to include a type of facial recognition. That information will upload to the cloud, as does Echo and Home.

SMART APPLIANCES

There are now household appliances that include smart technology programs and add a new level of control. Smart appliances can monitor, collect, and send data about their environment through Wi-Fi to the cloud, e.g., the LG Smart InstaView Door-in-Door refrigerator.

Amazon Echo and Google Home can be used with smart appliances. Alexa's integration allows you to search content and shop more efficiently by talking to your refrigerator. There is a camera that connects to your Wi-Fi so you can look inside from your phone or tablet. A feature called "smart tags" keeps track of items nearing or passing their "best if used by" dates. Data and photos upload to the cloud, similar to voice information transmitted by the personal assistant devices.

Other smart products include smart meters that have two-way communication with a utility and can communicate with appliances in the home. They may reveal usage, indicating what people are doing in their homes by sending information such as what appliances were being used, when, and how much.

In a recent case, a man was found dead in a hot tub at the residence of James Andrews Bates. Detectives observed that the hose had been used and the rim of the hot tub, deck, and surrounding items appeared to have been sprayed down. In the course of the investigation, police sought data from

the smart water meter and an Amazon Echo found in the home.

The court found the Amazon request overly broad, and Amazon did not produce any data from the Echo. However, the smart meter showed 140 gallons of water used between 1 a.m. and 3 a.m., which was determined to be far beyond normal. Prosecutors claimed the usage showed that the suspect hosed down his patio and hot tub and tampered with evidence. Bates claimed the water was used in the afternoon, not at night, and that the timer on the water meter was wrong. He said the water was used to fill the hot tub and not to hide evidence. He is set to go to trial next year for murder.

RECOVERABLE DATA

Because the microphones are always on or "listening" in these devices, the questions of what is being recorded, what is being used by the company, and what is recoverable need to be assessed. Users of personal assistants may not fully understand what data is being captured. For example, when Amazon Echo detects its wake word, it streams a "fraction of a second of audio before the wake word." That information goes to the cloud servers and is stored once your voice command is processed. According to Amazon, all of that gets saved with your main command.

Like the Echo, Google Home always listens, recording in short snippets and waiting for its wake word, such as the default "OK, Google." Once detected, a recording with its wake word is sent to Google's servers in the cloud. Amazon and Google keep these audio recordings of every voice command in their servers, which they claim are encrypted. It takes time and effort for a user to delete those recordings from the servers, and whether such consumer deletions are actually permanent and not recoverable at a later time is not currently proven.

Imagine a case where a fire is suspected to have involved a light and the lights in the home were controlled at the time by a personal assistant. An issue

becomes whether the lights were on or off at the time of a fire. A subpoena of Amazon or Google and the individual who used the personal assistant should be considered. That may reveal a stored command in support of testimony by a witness that the light was turned on or off. That is just one example since personal assistants can be used to perform many different functions.

Turning to the Samsung Otto prototype, this device has the added feature of a camera that can stream live video. Assume there is a fire in a room that contains this device. You'll want to know what data is set to upload and at what frequency it is uploaded to the cloud. It could be that the servers still have shots or video of the room where the fire occurred over time. It could show the condition of the room immediately before the fire, during the fire, or immediately after. A subpoena to not only Samsung, but also the server owner (if not Samsung) and the account holder should be considered.

The same analysis should be done for each smart appliance in the area of the incident being investigated. Recall the discussion about Bates' criminal case and the smart water meter. What data may be available? For example, the LG refrigerator has a camera. If one is present at a claim scene, did that camera capture and upload data that may be of use?

Since most assistants and smart appliances use apps on your phone or tablet, they likely will contain recoverable information. Those apps often can show a comprehensive overview of what a person does. Each request normally has a time stamp showing when the request was made, which could be used to establish if and when a person was in a particular room. For example, checking the Echo app on the individual's phone shows stored versions of requests made on the device.

PRIVACY CONSIDERATIONS

Personal assistant devices using microphones have been placed in

millions of homes—homes where adults and children live out of public view. Since the publication of “The Right to Privacy” by Samuel Warren and Louis Brandeis in the *Harvard Law Review* in 1890, critics have warned against the increasing ability of claims investigators to gather information previously thought to be private. That concern was further illuminated in George Orwell’s novel *Nineteen Eighty-Four*. And in his book *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, Edward Bloustein wrote that some see intrusions into another person’s privacy as the “primary weapon of the tyrant.”

The benefits of personal devices are obvious, but by using them, you are introducing a live microphone and data collection device into private and public spaces. To turn off Amazon Echo and Google Home, you must

manually turn off them off by pushing a physical button. These products generally use Wi-Fi to connect to the cloud. The recent presidential election involved claims that hackers accessed sensitive information not meant for public disclosure. Software can be hacked, manufacturers might not be truthful about their data collection activities/conduct (e.g., Volkswagen’s mileage claims), and speakers can be turned on surreptitiously. Hackers also can access the data being assembled and saved. Viable safeguards are needed. Anyone using smart products needs to weigh the pros and cons beforehand because they are voluntarily making a record that may be recoverable later.

Change is constantly happening to the products and services we use. Personal assistant devices and smart appliances offer great benefits while simultaneously generating data loaded

to the cloud and stored in servers.

For claims investigators, care should be taken to identify what personal assistant devices (Amazon Echo, Google Home, Samsung Otto, etc.) were in the area of concern. Were they used in connection with smart products like a Nest Cam, which can spot movement; Nest Protect, which can “smell” smoke and carbon monoxide; or Samsung Otto and LG Smart InstaView Door-in-Door refrigerator, which can take pictures or video. Efforts to preserve and obtain the data need to be assessed on losses going forward. One thing is certain, more and more data will continue to be collected, stored, and recoverable for losses now and in the future. ■

Peter A. Lynch is a vice chair and managing partner with Cozen O’Connor. He can be reached at plynch@cozen.com or follow him on Twitter @firesandrain.

Earning Your Trust One Claim at a Time. *That Will Never Change.*”

-William “Bubba” Ryan, CEO

Trust
RYTECH - The Industry Leader in
Water Mitigation & Mold Remediation.

We Do It Differently. We do it *better*- and our Insurance Industry Partners love us for the money we save them and the service we provide to their satisfied customers.



RYTECH Advantages

- Centralized Administration/ Call Center.
- IICRC, WRT and ASD certified field production staff on every job.
- Controlling Severity, from Rapid Response & Restoration to Cost Containment.
- **RYTRAC** In-Field Mobile Communications – Provides real-time overview to specific claims.



FRANCHISE OPPORTUNITIES AVAILABLE

1.800.865.8787 | RYTECHinc.com

