The People vs. Amazon Alexa: Connected Devices Are Not Hostile Witnesses

Christopher B. Hopkins | Wednesday, November 4, 2020

McDonald Hopkins member Christopher B. Hopkins recently had an article published by The American Bar Association.

The People vs. Amazon Alexa: Connected Devices Are Not Hostile Witnesses

A man in Fort Lauderdale, Florida, faces second-degree murder charges after his girlfriend was impaled with a spear that he kept by the foot of the bed. The criminal case made national news, not because of the bizarre circumstances of death, but due to the fact that Florida prosecutors had subpoenaed audio recordings from an Amazon Alexa device in the bedroom. During the upcoming trial, a jury may hear if Alexa recorded a crime. Is Alexa a new discovery tool for criminal and civil cases? How safe is it for lawyers to work at home or at the office with a smart device on their desks? What steps should you take to safely use an Alexa device (e.g., Amazon Echo) or other devices connected to the "Internet of Things"?

As tantalizing as it may be to pursue Alexa recordings as evidence in criminal and civil cases, to date Alexa has been a remarkably poor witness. That said, the mere issuance of a subpoena grabs headlines like, "Hey Alexa, Who Did It?" and "Alexa, Is He Guilty of Murder?" While provocative and amusing in the moment, the initial concept of Alexa providing evidence like that in the science fiction movie *Minority Report* appears so far to be a rush to judgment. In 2018, news outlets breathlessly reported that a search warrant was issued for Alexa recordings in a New Hampshire double murder, but two years later, evidence from Alexa was never introduced at trial. Before that, in 2017, a similar flurry of headlines resulted after county

prosecutors sought Alexa recordings in a death arising from a hot tub incident, but the recovered audio proved worthless. Dating back to 2014, news outlets incorrectly reported that a University of Florida student had asked Apple Siri where to bury his murdered roommate; however, those reports were inflated and misinformed. The victim was not a roommate and the evidence did not indicate that the accused had used Siri as an accomplice. Siri's previous response when asked where to dispose of a body (helpful suggestions such as "swamps," "reservoirs," "metal foundries," and "dumps") apparently had been a joke in the first place, but Apple quietly reprogrammed Siri to now respond, "very funny."

According to the probable cause affidavit in the pending Florida case, there is no reported reason to believe that Alexa was relevant in any way to the victim's untimely death other than being a device on the nightstand. In the five years since Amazon released its smart device, there are no reported criminal cases where Alexa actually recorded a crime.

Privacy and the Internet of Things

This does not suggest that "smart" or "connected" devices in our homes and offices could not leak information or provide evidence of a crime. We place myriad automated devices in our living and work spaces to monitor, record, and adjust our world. Cameras, doorbells, lights, baby monitors, thermostats, and even refrigerators are so widely connected that we have created an Internet of Things. This interconnectivity gathers, processes, and shares data about us, but it also creates several layers of risk. First, did you set up the device in a way that shares (only) an appropriate amount of information? Second, did you safely secure the device from potential third-party hackers? Third, does the manufacturer receive or share information gathered by your device, and is the manufacturer keeping that data safe?

Some readers may refuse to own an Amazon Alexa or Google Home device because of the perceived privacy risks. Let's take a quick test. Look around where you are sitting. How many cameras or microphones are in the room? In my office, I counted five microphones and four cameras sitting within arm's reach: On my desk there is a videoconference capable PC, laptop, iPad, iPhone, and an Alexa device. If you are reading this in a restaurant, lobby, conference room, or airplane, the amount of nearby recording devices might be enough to host a press conference. With that ubiquity comes a fear that someone is using technology to invade our privacy.

Here is another test. In the Google search bar, begin typing a search for "can someone remotely" and then pause. Google will dutifully offer to complete that sentence with suggestions such as "turn on my iPad camera," "access my computer camera," or "control my iPhone." Google's algorithm has been trained by the number of people who have asked these questions, and the answer is generally *yes*, any one of those devices could be spying on you. In 2016, a low-budget thriller *Ratter* depicted a single female student who moved to New York after a breakup only to be watched and terrorized by a hacker. The movie created a creepy tension because it was shot from the perspective of the woman's laptop and smartphone, so the audience had the voyeur's perspective. But it is not just hackers whom we fear.

Consumers are also afraid that corporations are spying on us. Class action plaintiffs have raised a number of complaints about Amazon's practices regarding preservation and use of voice recordings. Indeed, there are groups of *In Re Amazon.Com Alexa Cases* pending in northern California disputing these privacy concerns.

Still, it is misleading to believe that our privacy can be maintained by simply avoiding connected devices such as Alexa. The Internet of Things surrounds us, and it is hard to operate in a world without phones,

laptops, and tablets within arm's reach. When you visit someone's home or office, you probably will have no idea how connected the space is until your host demands, "Alexa, play smooth jazz!" As for your own living space, you may refuse to place an Alexa in your home "because it could be listening," but you have mistakenly overlooked that your smartphone is not in airplane-mode and that your other devices are connected to your WiFi. In today's world, if a device has a camera or a microphone, it also has an antenna, which means it is, or could, be sharing information about you. So how do we protect our privacy in a hyper-connected world?

Understanding Alexa's Privacy Protections

Alexa is constantly listening for its "wake word." Amazon, however, insists that it is not recording audio until it hears "Alexa!" In terms of connected devices, Alexa may be a relatively safe choice because, according to Amazon, it will always illuminate a blue ring (or a blue line on Echo Show devices) when recording, so you can visibly see it is listening. To turn off recording, you can hit the microphone button on top of the device, at which point the light will turn red. For the Echo Show 5 and 8, there is a shutter slide to block the camera.

You can always ask Alexa, "what was the last thing I said?" If Alexa pipes up unexpectedly, you can ask, "Alexa, tell me what you heard" or "Alexa, why did you do that?"

Five Steps to Fine-Tune Your Alexa Privacy Settings

The following steps will ensure that you have set up your device properly, protected yourself from hackers, and appropriately limited Amazon's use of your information.

1. Amazon provides an Alexa Privacy page, which can be found on Amazon.com (try this shortcut: https://amzn.to/3cNhSZg). You can also use the Amazon Alexa app, which you used to set up your devices in the first place. Using the latest version of the app, select "More" on the bottom right of the screen, then Settings, and then select Alexa Privacy. You will find that using the browser is easiest for the next three steps; however, the app is required for the final steps.
2. Let's satisfy your curiosity about what Alexa has been recording. On the Alexa Privacy page, tap "Review Voice History" and then extend the Date Range out a week or more. Scroll down to instances that are tagged "Audio was not intended for this device," and hit the down arrow to the right so you can then play the recording. Often, you will find these are failed instances where someone said "Alexa" but the sound was distant or there was overwhelming background noise. You can delete individual recordings or, back toward the top of the list, "Delete All Recordings for [this week]." Next, in the upper left corner, select "Review History of Detected Sounds," and, again, extend out the time period to a month or more. In my case, there were none. If there are sounds, you can choose to "Delete All Recordings."

   Before leaving that page, turn on "Enable Deletion by Voice." This allows you to verbally instruct, "Alexa, delete what I just said" or "Alexa, delete everything I said today." Coupled with the suggestions above, if you see the Echo's blue light or Alexa suddenly gives an unexpected response, you could ask Alexa to repeat what you just said and then give the command to delete any recorded audio.
3. Let's make sure that you have the proper Alexa privacy settings. Still on the Alexa Privacy page, select "Manage Your Alexa Data" in the upper left corner. Under "Manage Your Voice Recordings," you can choose to auto-delete recordings after three or 18 months or to do it manually. A conservative

approach might be to select 18 months. You also may choose to slide off both options to "Help Improve Alexa" (it has been suggested that Amazon employees are listening to recordings when these options are left on). While not recommended, you can "Manage Smart Home History," but that option essentially wipes all recordings and settings of your devices.

4. Recognize that Alexa maintains and shares data other than voice recordings. Back on the Alexa Privacy page, select "Manager Skill Permissions." In Amazon-speak, skills are different applications and services that run on your Alexa device. Make sure that third-party skills (or apps) do not have excessive permission rights. Click on each of the options starting with "Access Device Street Address" and make sure that all options are turned off unless you intentionally wish to give permission (after hitting each option, you will need to hit "Manage Skill Permissions" at the top of the screen because the back button does not work). Finally, go back to Review Voice History (from the Alexa Privacy page) and turn on "Enable Deletion by Voice" so that you can instruct Alexa to delete either what you just said or what was said all day.
5. Alexa devices can be used as an intercom inside your home as well as allow people to "drop in" or call other Alexa devices. Assuming that you do not use that feature, turn it off. Using the Alexa app, select "More" on the bottom right of the screen, select Settings, and then Device Settings. This will provide you a list of all Alexa-connected devices. For each Alexa device, tap on its name and then scroll down to tap Communications. From there, you can select which permissions to disable.

Five Steps for Securing Your Connected Devices

As mentioned above, the key to your privacy is to ensure that you limit the information a connected device can access, that you set it up securely, and that you understand how the manufacturer may be using your information. Every device has different settings and methods, but the following steps should help configure any connected device.

1. Determine whether your device is generally considered safe. Do a Google search for "[name of your device] + privacy" and carefully sift through the results. You might also substitute the words "privacy statement" to see if your device's manufacturer provides a plain English explanation of its practices.
2. Make sure the software or app is updated and that the device is running the current firmware.
3. Type the following as a Google search *with* the quotations: [name of your device] + "privacy settings". Among the search results, look for reliable sources such as the ABA, Forbes, Consumer Reports, and USA Today, as well as trusted tech sites such as CNET, Gizmodo, Ars Technica, and Tom's Hardware. Look for articles that give you step-by-step instructions on how to navigate and set your device's privacy settings.
4. Assuming the device is controlled by an app, look for the three horizontal lines or the spoke wheel to dig around in the settings for anything relating to privacy or reporting any information to the manufacturer. As a general rule, turn privacy settings to "on" and any self-reporting settings to "off."
5. For any device with a camera, including your laptop and webcam, consider a physical slide shutter. Do a Google or Amazon search for "camera privacy cover" or "camera cover slider" and the name of your device. For laptops, iPads, and other devices with small cameras, my favorite solution are these 6-pack plastic covers for $8.99 on Amazon (search for item number 8541707356).

Should My Law Firm Create a Policy?

As lawyers were forced to work remotely due to COVID-19, several large firms in March 2020 announced that they were banning employees from working near an Echo and other smart devices. Most jurisdictions

require lawyers to maintain strict client confidences and a certain level of competency with the technology we use in our daily practice. For the most sensitive data, obviously, lawyers should take the greatest precautions, and for all communications you should consider seclusion for conversations, shredding for paper copies, and encryption for digital files. However, as illustrated above, the news coverage of Alexa as a hostile witness has been overblown, and our scrutiny of connected devices overlooks the risks posed by the cameras and microphones in our phones, tablets, and laptops. Clear, consistent policies should require that users know how to set up and use their devices before deploying them, mandate the use of up-to-date software, and require careful adjustment of privacy settings. Instead of fearing connected devices, lawyers should use them properly to balance confidentiality and the benefits of the new technology.

Christopher B. Hopkins (chopkins@mcdonaldhopkins.com) is a privacy and cybersecurity lawyer with McDonald Hopkins LLC in West Palm Beach, Florida. In addition to his work in the courtroom, Mr. Hopkins' practice involves a wide range of emerging technologies such as privacy, defamation, Internet crimes, terms-of-service drafting, as well as OSINT, social media, and e-discovery.

Christopher B. Hopkins
Team member bio