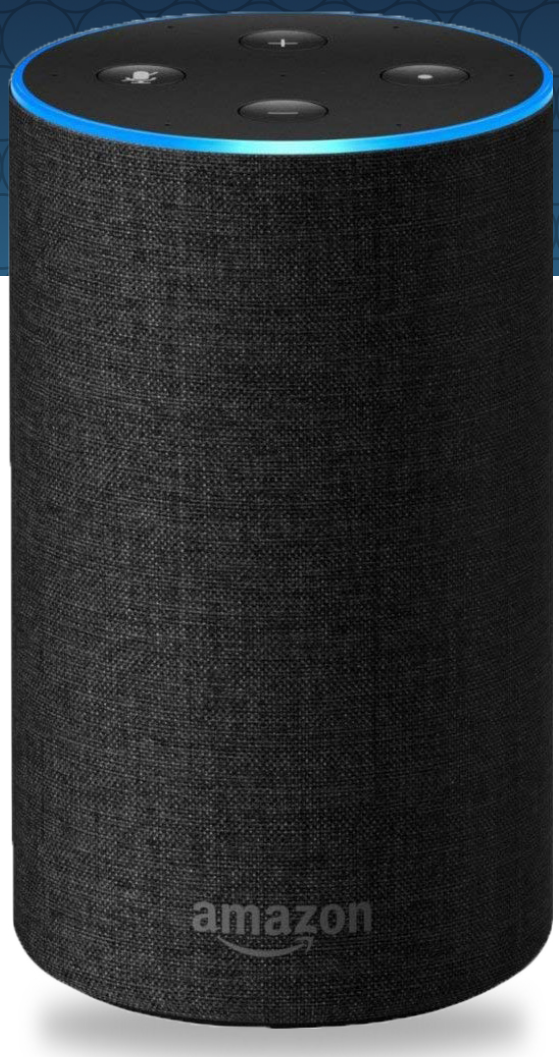
READ ARTICLE & EARN CLE

alexa, How did this happen?

Written by Amy H. Johnson and Vicki L. Kasper, ACP



As paralegals, we are constantly seeking information to get to the truth of the case. Today there are many sources of data to mine that we probably don't know existed that could help us gather information. It can be found in the technology we use every day.

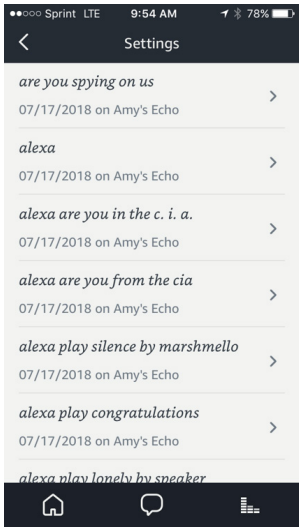
Much of the technology we use records our movements. For example, someone could track your activity based on your cell phone logs, internet browsing history, check-ins on social media, and even your Starbucks app. Your phone knows where you're going before you even get there, and getting access to Waze data will determine vehicle speed or route changes for a particular driver.

As technology has become more integral to daily life, authorities have increasingly sought evidence from mobile phones, laptops, social media, even online video games. Attempting to mine a smart speaker for information is likely an up and coming subpoena template.

Artificial Intelligence (AI) is a term first coined by John McCarthy in 1956, where he defined it as "the study and design of intelligent agents." Today the term is used more broadly to describe computer systems that perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages. In common terms this »

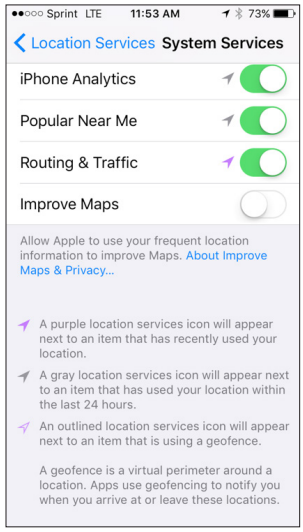
means facial recognition, fingerprint scanning, algorithms used by eBay and Amazon Marketplace to adjust the sellers' prices, traffic routing, thermostats that sense and adapt to motion, and many other functions that society now takes for granted as routine parts of daily life. Most industries increasingly identify areas where the use of artificial intelligence can maximize efficiency, including healthcare, manufacturing, fast food, and the financial sector. Law offices are no exception. Rather than discuss how individual law firms can implement AI for daily tasks, this article will focus on using data mined from AI – for good or for bad.

If you have Alexa in your home (or Siri, Google Assistant, or Cortana), did you know that when you say the wake word, the device starts recording? The audio is transported to the cloud and stays there until you actively delete it. If you're worried about what Alexa has recorded in your home, you can easily find out. Open the Alexa app (you needed to install this app on your smartphone to initially pair the Alexa speaker) and click the menu on the left side. Select Settings and scroll down to History. You can read your phrases, play back the original recording, and delete them.



As you peruse the History, you may learn the music your husband requested at 7 a.m. or questions your kids asked when you weren't home. You will hear the actual recording, including any background noise. It's pretty creepy. Be sure to listen to the entries that say "text is not available" because as tempted as you may be to scroll past those, it actually indicates an instance when Echo was awakened with the wake word and recorded something that was not a request.

There are many other examples where AI is recording your activities that you may not know. If you have your smartphone's wi-fi turned on, then each time you pass a store or other business with wi-fi, your smartphone might be pinging the network and your location could be recorded. That's right, if you are walking along the National Mall in D.C. with your phone's wi-fi enabled or using Google maps to find your next destination, someone monitoring your location history may infer that you made quick dashes to graffiti the Smithsonian, Pete's Hot Dog Stand, and so many other locations when in reality you were innocently strolling along with your toddler.



Your personal iPhone also keeps tabs on your whereabouts and frequently used apps, but doesn't necessarily share the information with Apple. If you have ever noticed a bar across the bottom of your iPhone that recommends a certain app based on your location, then be warned that your location privacy settings are very permissive. For example, if you sit down in that comfy chair in your sunroom and you see a bar suggesting Word Scramble, your iPhone is using location services with the data analytics. To read more about this feature on the iPhone or to adjust your smartphone's settings, check out this article: https://www.cultofmac.com/522515/how-to-see-iphone-significant-locations-map/

If you use Waze to speedily navigate your morning commute, be aware that data is stored. Think of all the information Waze could capture – your speed, starting and ending points, stops made along the way, and even the music you listened to en route. Another app, Life360, is a useful family location sharing tool. It too records driving habits including sudden accelerations, hard braking, and phone usage while the vehicle is moving.

Consider possible uses of the information for litigation cases. Let's say your firm is defending a large trucking company where one of its drivers allegedly caused a fatal collision on a rural highway. Your driver swears he kept accurate log books, rested when he was supposed to, and obeyed the traffic laws during the 48 hours leading up to the collision. He maintains the passenger vehicle abruptly changed lanes in front of him and he had no chance to avoid the collision. Because it was a desolate stretch of road and the accident occurred in the wee hours of the morning, there were no eyewitnesses. How do you prove your driver's version of the events? Try to get as much AI as exists – from your driver a well as the other vehicle. Presumably the adverse party(ies) is in the vehicle your truck driver hit. It's easy to start with imaging the electronic data modules for both vehicles, but typically those devices begin recording vehicle movements and inputs only moments prior to a triggering event (i.e. the collision). Consider an interrogatory seeking to identify all mapping programs and route guidance utilized in the passenger vehicle for the four days before and after the collision, or a Request to Inspect »

all cellular phones and other electronic devices present in the vehicle when the collision occurred. A computer and mobile forensics expert can image the devices and potentially uncover useful information.

Here's another one: Let's say you are tasked with poking holes in a witness's statement about a crime they claim to have witnessed. In addition to standard background checks, character investigations, and traditional physical evidence, is there evidence you can gather from AI sources?

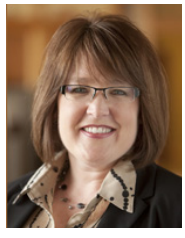
Now that you have identified AI sources you'd like to mine, how do you obtain the data? One possibility is simply to ask the owner. If the owner is an adverse party (or employee of the adverse party), send a spoliation letter early to prevent destruction or deletion of stored information, and then at the appropriate time ask the owner for permission to inspect or image the device. This tactic is only as good as the repository of data stored on the actual device. For example, Amazon says Alexa stores short voice recordings, usually 30 seconds, on the actual device that sits in someone's home. Other recordings, if they exist, are stored in the cloud. So demanding to inspect the actual Alexa device is unlikely to reveal a treasure trove of usable data.

Cell phones, on the other hand, contain terabytes worth of data that can even include data the user thought was deleted. You will need a certified forensic expert to retrieve the data and preserve the chain of custody. Some experts may include John Akerman at www.rosenltc.com, or Gavin Manes, PhD at www.avansic.com. For other programs that store data in the cloud, ask the owner to provide login and password information to view the user history on apps such as Waze and Life360 that were mentioned in this article. If that is not possible or the owner refuses reasonable access, consider sending a subpoena. The reality of obtaining this data through subpoena power is still unknown. In a recent murder case (*State of Arkansas v. James A. Bates*, Case No. 2016-370-2 (Ark. Cir.)), even though the defendant agreed to turn over Echo's Alexa recordings, Amazon moved to quash the subpoena based on privacy laws. Some speculate it's because Amazon fears this is a slippery slope that will open the door to privacy invasion and a general onslaught of fishing expeditions into the data utilized by AI. That same case also tapped data recordings from another smart device in the home, the hot water heater. Don't let this deter you though; be assured that Amazon and Google won't respond to 100% of the subpoenas you don't serve.

For more information about where to serve a subpoena on Google in a civil case, go here: https://support.google.com/faqs/answer/6151275?hl=en. And for Amazon, go here: https://associatesmind.com/2013/04/24/how-to-subpoena-amazon/

If you've read this far, keep an eye out for potential AI evidence you can uncover in the cases you work every day. Be creative, and back up your requests with solid reasons as to why the information is potentially useful. When the first 911 call was made in 1968 in Haleyville, Alabama, it was unlikely that the National Association of Fire Chiefs, or the Alabama Telephone Co. could have imagined how the emergency call process would evolve. Today obtaining recordings of 911 audio is commonplace in every wreck case, mainly because early calls weren't even recorded, and then when recordings began the stations used cumbersome equipment where culling out one call required unwieldy time and effort, not to mention the obstacles associated with producing a duplicate copy of the call. Today, however, those very valuable audio files can be harvested with a simple email to and from the dispatch center, accompanied by the appropriate authorization permitting their release. Perhaps in our lifetime, mining AI data will follow the same course. Only time – and possibly Alexa – will tell.

Amy H. Johnson is employed as a senior paralegal at the law firm of Yarborough Applegate LLC, in Charleston, SC where she specializes in catastrophic personal injury, wrongful death, and complex civil litigation. She is an active member of Charleston Association of Legal Assistants, where she has served as President, NALA Liaison, Education Chair, and Parliamentarian. She currently serves on NALA's Ethics Committee. She was awarded the American Association For Justice (AAJ) National Paralegal of the Year in 2017 and is a frequent presenter at continuing education events nationwide. ✉ *amy@yarboroughapplegate.com*



Vicki L. Kasper, ACP, is employed as a paralegal for Sizzling Platter, LLC, a restaurant management company. Ms. Kasper earned her B.S. degree from the ABA approved Paralegal Program at Minnesota State University Moorhead in Moorhead Minnesota. She earned her CP designation in 2010 and her ACP designation in 2014 for Business Organizations: Incorporated Entities. She is past President of the Red River Valley Paralegal Association, former Continuing Education Council member and currently the NALA Ethics Committee Chair and NALA Liaison for Utah Paralegal Association. ✉ *vkasper@phillipsedison.com*