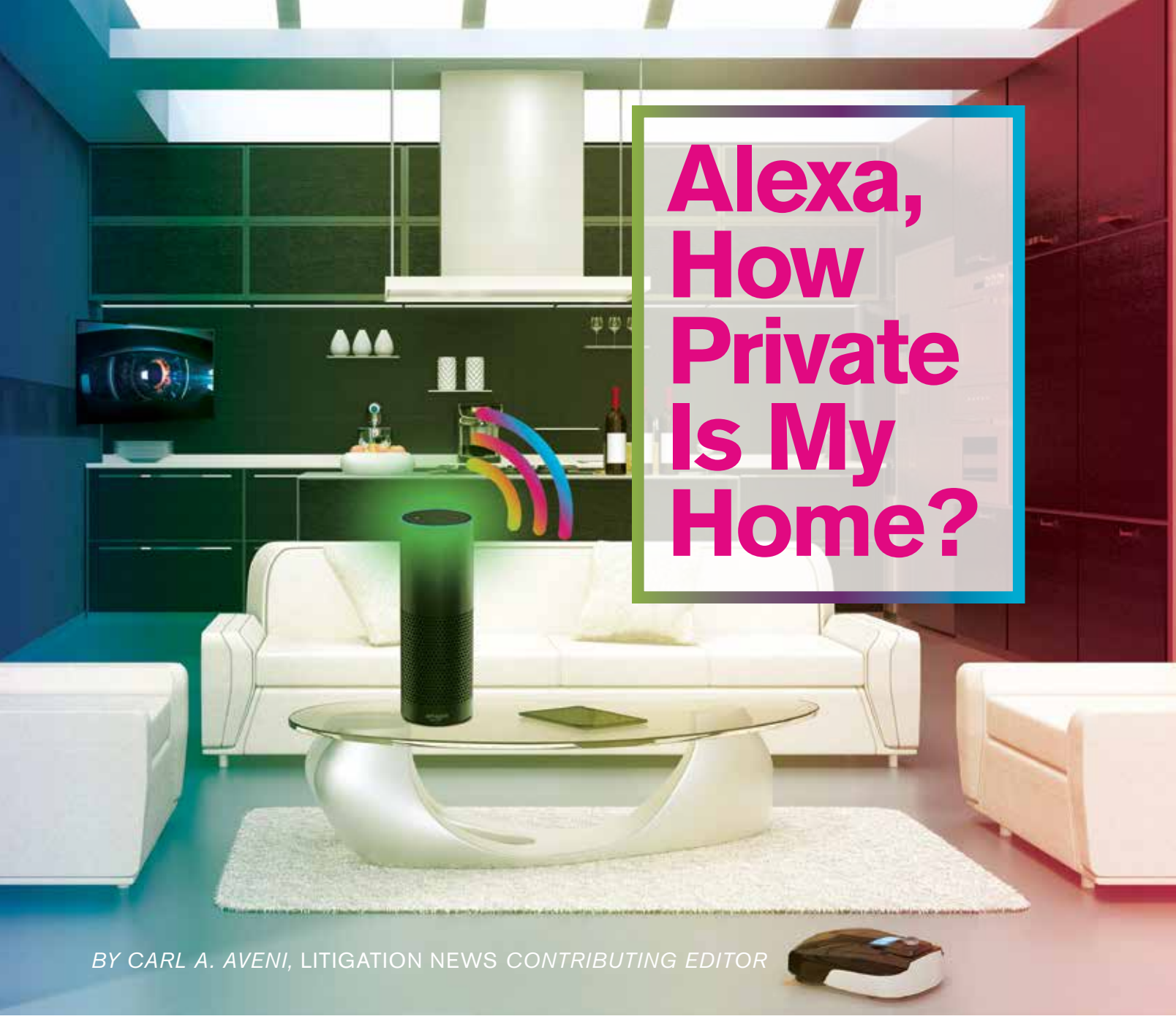

Alexa, How Private Is My Home?

BY CARL A. AVENI, LITIGATION NEWS CONTRIBUTING EDITOR

© ISTOCK

Alexa. Cortana. Siri.

Odds are good that you own devices connected to at least one of these voice-activated digital assistants. A phone in your pocket. A laptop on your desk. Perhaps a smart TV or an Amazon Echo sitting somewhere in your home. Convenient to use, perhaps, but also omnipresent. Listening. Collecting both your active search requests and all of the accompanying ambient sounds of your household, for streaming and storage in the cloud. As these voice-activated devices become ubiquitous, new questions are emerging about how this technology changes traditional notions of privacy—and the trade-off between convenience and confidentiality.

Amazon has staked new ground at the center of this debate. Faced with a search warrant for access to a customer's voice and search data as part of a murder investigation, Amazon asserted that the responsive materials were protected by the First Amendment. A novel response to a recurring question, as lawyers and judges struggle to catch up with technological change.

MURDER, SHE SPOKE

Victor Collins was found dead in a hot tub at the Bentonville, Arkansas, home of his friend, James Bates, on November 22, 2015. Bates had invited Collins and several other friends over for a night of drinking and football. After the other friends left around 1:00 a.m., Bates claims to have retired to sleep. He purportedly awoke hours later to find Collins face down in the hot tub. After Bates called 911, detectives determined that Collins had died primarily of strangulation, not drowning. Collins's body was bleeding, and the room had signs of both a struggle and cover-up. Bates's phone showed multiple failed calls throughout the night, at times when Bates claimed to have been asleep. Bates himself had bruises and scratches that he could not account for. And utility records showed an increase in water usage, perhaps to wash down the scene and eliminate evidence. Unfortunately, there were no other witnesses to testify about what they heard at the time of the murder. But Bates had an Amazon Echo device, running its Alexa digital assistant software, right at the scene of the crime.

The Amazon Echo is a hands-free voice-controlled digital speaker. It uses a processor to identify a "wake word" that when triggered connects the device to Amazon's cloud-based Alexa voice service. Because the device is always on and streams to the cloud not just processed requests and responses but also contemporaneous ambient sounds, Alexa might well have recorded details associated with the murder. The police issued a warrant for all data recorded over the 24 hours surrounding the murder. Amazon filed a motion to quash, urging that the warrant violated the First Amendment rights of both its customer and of Amazon itself.

SPEECH, PERHAPS, BUT WHO IS THE SPEAKER?

According to Amazon, "the heart of the First Amendment protection is the right to browse and purchase expressive materials anonymously, without fear of government discovery." Analogizing to earlier cell phone case law, Amazon asserted that Alexa contains "a multitude of data that can reveal much more in combination than any isolated record, allowing those with access to reconstruct 'the sum of an individual's private life.'" The data includes both the consumer's search requests and Amazon's ordering of potential responses and results—each of which contains expressive content under the First Amendment. For example, Amazon argued, "users may ask for information about a sensitive health condition or a controversial political figure. Users can now order products from Amazon, including books and other expressive materials, using the Alexa Voice Service." Accordingly, Amazon cited earlier search engine case law that "the fear of government tracking and censoring one's reading, listening, and viewing choices chills the exercise of First Amendment rights." From that perspective, Amazon claimed, the search requests of its customers are entitled to heightened First Amendment protection from government intrusion.

Amazon asserted that Alexa's own responses to those search requests are equally protected, analogizing to the U.S. District Court for the Southern District of New York's conclusion that "the First Amendment protects as speech the results produced by an Internet search engine." Alexa's decision algorithms about what information to include in its response, like the ranking of search results, is "constitutionally protected opinion" that is "entitled to 'full constitutional protection,'" Amazon argued.

Relying on earlier search engine case law, Amazon maintained that the warrant must be quashed, unless the government made a heightened showing of relevance and need for the data. Specifically, the state must demonstrate (1) a compelling need for the information sought, including that it is not available from other sources; and (2) a sufficient nexus between the information and the subject of the criminal investigation. As Amazon noted, courts applying this test in other contexts have concluded "law enforcement officials' need for the information sought cannot be compelling if there are reasonable alternative ways of conducting an investigation," and "officials must exhaust these alternatives before resorting to techniques that implicate fundamental expressive rights."

SKEPTICS RESPOND WITH SPEECH OF THEIR OWN

Not everyone is convinced. "Purely private personal expression has always been discoverable, even in civil litigation, under the right circumstances. Diaries, for example, are often discoverable—to say nothing of social media posts," says Marcus R. Chatterton, Birmingham, AL, cochair of the ABA Section of Litigation's Intellectual Property Litigation Committee. "The First Amendment argument is not a perfect fit. It's true that by obtaining this sort of passive information, the government could have a chilling effect. But, it's not going to be a chilling effect on people saying or doing things in their home," Chatterton adds. "It would be a chilling effect on people using Amazon's device. So the chilling effect is not that it's going to prevent the speech. It's going to prevent the speaker from using that particular commercially available technology."

Abraham Y. Skoff, New York, NY, cochair of the Trade Secrets Subcommittee of the Section of Litigation's Business Torts & Unfair Competition Committee, agrees. "If what is being protected is really the company's interest in maintaining this consumer relationship and protecting a

commercial asset, or in profiting from its ability to collect this type of data, I think that a court will see that as a less significant interest than even corporate free speech writings," Skoff explains, noting that commercial speech has historically received lesser First Amendment protection.

WHAT HAPPENS ON ALEXA STAYS ON ALEXA

Even so, "Amazon is onto something, however. These recordings from inside the home shouldn't be easily obtainable," Chatterton notes. "But so far, the legal framework to protect private consumer information hasn't kept up with technology's ability to capture it." Even if the legal framework is underdeveloped, however, the commercial imperative was obvious. "It's absolutely critical, from a business perspective, for Amazon and every other company in the consumer technology space, to plant a flag and protect their customers' data privacy," Chatterton observes, adding that "if they don't plant the flag here, they're going to see a real drop in customers willing to adopt their technologies."

Chatterton is not alone in thinking so. "This is an important case for consumers because it's one of the first to test how well our privacy rights will stand up to the new networked world in which we live," says James W. Cobb, Atlanta, GA, cochair of the Trade Secrets Subcommittee of the Section's Business Torts & Unfair Competition Committee. "Lawyers, judges, and consumers are starting to wrestle with whether our smart devices—our coffee machines, our refrigerators, our televisions—can be forced into service as government informants," Chatterton adds, noting that the stakes couldn't be more serious, either for business or for consumer privacy. "These concerns will only multiply, as smart devices become more ubiquitous in our homes."

Skoff shares this worry. "We're only a short couple steps away from one's residence essentially knowing almost everything about what a person is doing. Not just what music they're listening to or what newspaper articles they're reading, but every part of every minute of their lives," he explains. "What happens to privacy when the government, a company, or some third party can use the Internet and devices like Alexa to virtually reconstruct every single thing a person did all day long, from morning to night? What privacy is left?"

OLDER STANDARDS STILL APPLY

Others take a different view. For Anthony J. Carriuolo, Fort Lauderdale, FL, cochair of the Social Media & Website Subcommittee of the Section's Business Torts & Unfair Competition Committee, there is already a remedy to any constitutional privacy concerns. "The question of whether or not the government can access information generated or gathered by that device is, in my view, a separate Fourth Amendment issue having nothing to do with the commercial interaction for which the customers initially brought the device into their home," Carriuolo explains. "The government's ability to gather any citizen information—whether it be on a hand-held dictaphone, a wiretap, or gathered by Alexa and stored in the cloud—is subject to the same constitutional analysis. There should be no difference in outcome simply because of advances in the technology by which the statements were gathered and stored."

Indeed, Carriuolo wonders whether the privacy concerns have become a bit overblown. As he notes, "this is a commercially generated experience that consumers have elected to bring into the privacy of their homes. And those consumers interact voluntarily and intentionally with it. So I think the Orwellian concerns that have been mentioned in some media don't fit the commercial realities posed by Alexa and Siri and other artificial intelligence interactives." For him, the existing search and seizure standards applied to protect citizens in other contexts are amply up to the job posed by digital assistants. "I would continue to vigilantly assert the rights to protect consumer data against government intrusion, and require the government to meet the standards under the Fourth Amendment," Carriuolo explains.

CHANGES TO THE PRACTICE

Cobb worries at least as much about how these emerging technologies will change the business and practice of law. He recites a list of discovery questions lawyers should pose to clients in this new era: "Do you use a digital personal assistant that is affiliated with a cloud provider? What are the terms and conditions of your arrangement with that cloud provider? Do you have control, possession, or custody over the data that sits within that cloud provider's servers? Or does the cloud provider have that control?"

He continues, "If I'm representing a company in a trade secret dispute, and the other party has an Echo in the board room, I'm now going to ask for that Echo's data in discovery. I'll include it in a litigation hold notice. I'll make sure they don't delete anything from Alexa. And if folks are sitting around in a conference room, and Alexa picks up a snippet of conversation related to the trade secret, I've got an argument now that they haven't taken adequate steps to protect the confidentiality of their alleged trade secret. Maybe it's not a trade secret anymore."

Indeed, these issues may also affect the business of law every bit as much as the substantive representations, Cobb notes, thinking about the increasing number of firms that use cloud-based document storage systems. "Some of the issues we face in terms of managing the risk to the firm are similar to the risks that a consumer might face, because a third-party company that hosts the cloud system now has some measure of control over our data."

Under a strict interpretation of ABA Model Rule 1.6, the mere fact that a lawyer represents a client is itself confidential information, Cobb observes. And yet, if a lawyer uses a cloud-based digital assistant for calendaring or document

The digital revolution is changing the way that lawyers and police gather evidence. Here are a few recent examples of technology shaping arguments in the courtroom.

amazon

Online e-book purchases subject to First Amendment protection.

Amazon.com, LLC v. Lay, 758 F. Supp. 2d 1154 (W.D. Wash. 2010).

http://bit.ly/amazon-lay

Baidu 百度

Internet search engine permitted to exercise editorial control over ranking of results under First Amendment.

Zhang v. Baidu .com, Inc., 10 F. Supp. 3d 433 (S.D.N.Y. 2014).

http://bit.ly/zhang-baidu

fitbit

Fitbit data led Connecticut police to arrest a man in connection with his wife's death.

Connecticut v. Richard Dabate, TTD-CR17-0110576 (Conn. 2017).

http://bit.ly/bondarenko-fitbit

Cellphone passcode not entitled to constitutional protection.

Florida v. Voigt, No. F16015256, (Fla. Cir. Ct. 2017) (orally granted May 3, 2017).

http://bit.ly/florida-voigt

storage, that information has effectively been shared with the service provider. "A lot of lawyers might not think about the implications of that," Cobb worries. "As the adoption rate of cloud-based technology increases, I think these are issues that are going to come to the forefront of the business of practicing law."

The solution may require the law firms to exercise greater diligence with their vendors. "If I decide to use Amazon Echo in my business, I might need to consider going to Amazon and looking at the terms and conditions that are associated with my use of the Echo and, if they're not sufficiently protective, I might need to negotiate for some more stringent confidentiality protection."

WHAT TOMORROW HOLDS

Some of these issues will have to wait for a future case to test their parameters. After Amazon filed its motion to quash, Bates, the criminal defendant, voluntarily waived his own objections and turned his Alexa data over to the prosecutors. In light of that waiver, Amazon withdrew its motion. But few doubt that the issue will arise again, as digital assistants assume a broader role in daily life. "I think you're going to continue to see these types of issues raised alongside the proliferation of these types of artificial intelligence devices and activities," Carriuolo acknowledges. "Over the past few years, many more folks have come to realize that nothing's private. Everything is being heard, everything is being recorded, and everything is being seen. That's true for outside the home. And with the technologies we invite in for our own purposes, that's increasingly true inside the home as well."

Chatterton agrees. "Whether it's realistic or not, some people fear that they are going to wake up like Jim Carrey in *The Truman Show* and suddenly realize that their whole lives are being recorded," he adds ruefully.

Skoff is more hopeful that evolving technology may solve the problem that it also created: "Maybe a 'Snapchat of the Internet of Things'—where they gather the information, distill it to the extent they need it, but then automatically delete it in 20 days. So that if they are subpoenaed within a short period of time, the data is there. But if the subpoena comes later, the data is gone. At least that way, people wouldn't feel like *Big Brother* is always looking over their shoulder at what they've been doing."

Carriuolo has a slightly different take. "Amazon has been able to convert what was a pretty straightforward criminal prosecution of a customer into a broad marketing campaign for the Amazon Alexa," he observes, before laughing. "This is great and arguably free promotion for Amazon and its Alexa product. Regardless of the outcome of the prosecution of the case in which these issues were raised, Amazon is clearly a winner in the marketplace."

RESOURCES

- *Arkansas v. James Bates*, No. CR-2016-370-2 (Benton Cty., AR, 2017).
- Debra C. Weiss, "Alexa's Responses to Customers Are Protected by the First Amendment, Amazon Argues in Murder Case," *ABA J.*, Feb. 27, 2017, available at http://bit.ly/aba-weiss-amazon.
- Veronika Bondarenko, "Police Pieced Together That a Husband May Have Murdered His Wife Based on Her Facebook Posts and Fitbit Data," *Business Insider* (Apr. 26, 2017), available at http://bit.ly/bondarenko-fitbit.
- Robert T. Denny, "Warrantless Search of Cell Phone Violates Fourth Amendment," *Litigation News* (May 5, 2016), available at http://bit.ly/Denny-050516.