BUSINESS LAW TODAY

"Alexa, Do You Have Rights?": Legal Issues Posed by Voice-Controlled Devices and the Data They Create

By Eric Boughman, Sara Beth A.R. Kohut, David Sella-Villa, and Michael V. Silvestro

The decision to use voice-controlled digital assistants, like Amazon's Alexa, Apple's Siri, Microsoft's Cortana, and the Google Assistant, may present a Faustian bargain. While these technologies offer great potential for improving quality of life, they also expose users to privacy risks by perpetually listening for voice data and transmitting it to third parties.

Adding a voice-controlled digital assistant to any space presents a series of intriguing questions that touch upon fundamental privacy, liability, and constitutional issues. For example, should one expect privacy in the communications he engages in around a voice-controlled digital assistant? The answer to this question lies at the heart of how Fourth Amendment protections might extend to users of these devices and the data collected about those users.

Audio-recording capabilities also create the potential to amass vast amounts of data about specific users. The influx of this data can fundamentally change both the strength and the nature of the predictive models that companies use to inform their interactions with consumers. Do users have rights in the data they generate or in the individual profile created by predictive models based on that user's data?

On another front, could a voice-controlled device enjoy its own legal protections? A recent case questioned whether Amazon may have First Amendment rights through Alexa. Whether a digital assistant's speech is protected may be a novel concept, but as voice-controlled digital assistants become more "intelligent," the constitutional implications become more far-reaching.

Further, digital assistants are only one type of voice-controlled device available today. As voice-controlled devices become more ubiquitous, another question is whether purveyors of voice-controlled devices should bear a heightened responsibility towards device users. Several security incidents related to these devices have caused legislators and regulators to consider this issue, but there remains no consensus regulatory approach. How will emerging Internet-of-Things frameworks ultimately apply to voice-controlled devices?

Voice-Activated Digital Assistants and the Fourth Amendment

Voice-activated digital assistants can create a record of one's personal doings, habits, whereabouts, and interactions. Indeed, features incorporating this data are a selling point for many such programs. Plus, this technology can be available to a user virtually anywhere, either via a stand-alone device or through apps on a smartphone, tablet, or computer. Because a digital assistant may be in perpetual or "always-on" listening mode (absent exercise of the "mute" or "hard off" feature), it can capture voice or other data that the user of the device may not intend to disclose to the provider of the device's services. To that end, users of the technology may give little thought to the fact their communications with digital assistants can create a record that law enforcement (or others) potentially may access by means of a warrant, subpoena, or court order.

A recent murder investigation in Arkansas highlights Fourth Amendment concerns raised by use of voice-controlled digital assistants. While investigating a death at a

private residence, law enforcement seized an Amazon Echo device and subsequently issued a search warrant to Amazon seeking data associated with the device, including audio recordings, transcribed records, and other text records related to communications during the 48-hour period around the time of death. *See State of Arkansas v. Bates*, Case No. CR-2016-370-2 (Circuit Court of Benton County, Ark. 2016).

Should one expect privacy in the communications he engages in around a voice-activated digital assistant? The Arkansas homeowner's lawyer seemed to think so: "'You have an expectation of privacy in your home, and I have a big problem that law enforcement can use the technology that advances our quality of life against us.'" Tom Dotan and Reed Albergolti, "Amazon Echo and the Hot Tub Murder." The Information (Dec. 27, 2016) (hereinafter "Dotan").

To challenge a search under the Fourth Amendment, one must have an expectation of privacy that society recognizes as reasonable. With few exceptions, one has an expectation of privacy in one's own home, *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001), but broadly, there is no reasonable expectation of privacy in information disclosed to a third party. Any argument that a digital-assistant user has a reasonable expectation of privacy in information disclosed through the device may be undercut by the service provider's privacy policy. Typical privacy policies provide that the user's personal information may be disclosed to third parties who assist the service provider in providing services requested by the user, and *to third parties as required to comply with subpoenas, warrants, or court orders*.

The *Bates* case suggests that data collected by digital assistants would bear no special treatment under the Fourth Amendment. The police seized the Echo device from the murder scene and searched its contents. Unlike a smartphone that would require a warrant to search its contents, *see Riley v. California*, 134 S. Ct. 2473, 2491 (2014), the Echo likely had little information saved to the device itself. Instead, as an Internet-connected device, it would have transmitted information to the cloud, where it would be processed and stored. Thus, the Arkansas law enforcement obtained a search warrant to access that information from Amazon.

Under existing law, it is likely a court would hold that users of voice-activated technology should expect no greater degree of privacy than search engine users. One who utilizes a search engine and knowingly sends his search inquiries or commands across the Internet to the search company's servers should expect that the information will be processed, and disclosed as necessary, to provide the requested services.

Perhaps there is a discernible difference in that voice data, to the extent a service provider records and stores it as such, may contain elements that would not be included in a text transmission. For example, voice data could reveal features of the speaker's identity (such as a regional accent), state of mind (such as excitement or sadness), or unique physical characteristics (such as hoarseness after yelling or during an illness), that would not be present in text.

Or perhaps it is significant that some information transmitted might enjoy a reasonable expectation of privacy but for the presence of the device. Although digital-assistants usually have visible or audio indicators when "listening," it is not inconceivable that a digital assistant could be compromised and remotely controlled in a manner contrary to those indicators.

Further, the device could be accidentally engaged, particularly when the "wake word" includes or sounds like another common name or word. This could trigger clandestine or unintentional recording of background noises or conversations when the device has not been otherwise intentionally engaged. *See* Dotan ("[T]he [Echo's seven] microphones can often be triggered inadvertently. And those errant recordings, like ambient sounds or partial conversations, are sent to Amazon's servers just like any other. A look through the user history in an Alexa app often reveals a trove of conversation snippets that the device picked up and is stored remotely; people have to delete those audio clips manually.").

The technology of voice-activated digital assistants continues to advance, as evidenced by the recent introduction of voice-controlled products that include video capabilities and can sync with other "smart" technology. Increasing use of digital assistants beyond personal use will raise more privacy questions. As these devices enter the workplace, what protections should businesses adopt to protect confidential information potentially exposed by the technology? What implications does the technology have for the future of discovery in civil lawsuits? If employers utilize digital assistants, what policies should they adopt to address employee privacy concerns? And what are the implications under other laws governing electronic communications and surveillance?

First Amendment Rights for Digital Personal Assistants?

The *Arkansas v. Bates* case also implicates First Amendment issues. Amazon filed a motion to quash the search warrant, arguing that the First Amendment affords protections for both users' requests and Alexa's responses to the extent such communications involve requests for "expressive content." The concept is not new or unique. For example, during the impeachment investigation of former President Bill Clinton, independent counsel, Kenneth Starr, sought records of Monica Lewinsky's book purchases from a local bookstore. *See In re Grand Jury Subpoena to Kramerbooks & Afterwords Inc.*, 26 Media L. Rep. at 1599 (D. D.C. 1998).

Following a motion to quash filed by the bookstore, the court agreed the First Amendment was implicated by the nature of expressive materials, including book titles, sought by the warrant. Ms. Lewinsky's First Amendment rights were affected, as were those of the book seller, whom the court acknowledged was engaged in "constitutionally protected expressive activities." Content that may indicate an expression of views protected by free speech doctrine may be protected from discovery due to the nature of the content. Government investigation of one's consumption and reading habits

is likely to have a chilling effect on First Amendment rights. *See U.S. v. Rumely*, 345 U.S. 41, 57-58 (1953) (Douglas, J., concurring); *see also* Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2002) (protecting consumer records concerning videos and similar audio-visual material).

Amazon relied on the Lewinsky case, among others, contending that discovery of expressive content implicating free speech laws must be subject to a heightened standard of court scrutiny. This heightened standard requires a discovering party (such as law enforcement) to show that the state has a "compelling need" for the information sought (including that it is not available from other sources) and a "sufficient nexus" between the information sought and the subject of the investigation.

The first objection raised by Amazon did not involve Alexa's "right to free speech," but instead concerned the nature of the "expressive content" sought by the Echo user and Amazon's search results in response to the user's requests. The murder investigation in question, coupled with the limited scope of the request to a 48-hour window, may present a compelling need and sufficient nexus that withstands judicial scrutiny.

However, Amazon raised a second argument that Alexa's responses constitute an extension of Amazon's own speech protected under the First Amendment. Again, the argument is supported by legal precedent.

In *Search King, Inc. v. Google Tech., Inc.*, an Oklahoma federal court held that Google's search results were constitutionally protected opinion. 2003 WL 21464568 (W.D. Okla. 2003). More recently, a New York federal court determined that Baidu's alleged decision to block search results containing articles and other expressive material supportive of democracy in China was protected by the First Amendment. *Jian Zhang v. Baidu.com, Inc.*, 10 F.Supp.3d 433 (S.D.N.Y. 2014). Accordingly, no action could lie for injunctive or other relief arising from Baidu's constitutionally protected decisions.

The court considered search results an extension of Baidu's editorial control, similar to that of a newspaper editor, and found that Baidu had a constitutionally protected right to display, or to consciously not display, content. The court also analogized to a guidebook writer's judgment about which attractions to feature or a political website aggregator's decision about which stories to link to and how prominently to feature them.

One unique issue that arises in the context of increasingly "intelligent" computer searches is the extent to which results are not specifically chosen by humans, but instead returned according to computer algorithms. In *Baidu*, the court was persuaded by the fact that the algorithms are written by humans and thus "inherently incorporate the search engine company engineers' judgments about what materials" to return for the best results. By its nature, such content-based editorializing is subject to full First Amendment protection because a speaker is entitled to autonomy to choose the content of his message. In other words, to the extent a search engine might be considered a "mere conduit" of speech, First Amendment protection might be less (potentially subject to intermediate scrutiny), but when the search results are selected or excluded because of the content, the search engine, as the speaker, enjoys the greatest protection.

Search results arising from computer algorithms that power search engines and digital assistants may currently be considered an extension of the respective companies' own speech (through the engineers they employ). Current digital assistants are examples of "weak artificial intelligence." Thornier legal questions will arise as the artificial intelligence in digital assistants gets smarter. The highest extreme of so-called "strong" artificial intelligence might operate autonomously and be capable of learning (and responding) without direct human input. The First Amendment rights of such systems will no doubt be debated as the technology matures.

Voice Data and Predictive Models

Digital assistants have the potential to gather massive amounts of data about users. Current voice data analytic tools can capture not only the text of human speech, but also the digital fingerprint of a speaker's tone, intensity, and intent. Many predictive models rely extensively on lagging indicators of consumption, such as purchases made. Voice data might be able to provide companies with leading indicators, such as information about the user's state of mind and triggering events that may result in the desired interactions with a company.

Incorporating voice data into current predictive models has the potential to make them vastly more accurate and specific. A digital assistant might record and transmit the message "Pat is going to the hospital for the last time." Based on only text of the message, an algorithm might predict that a tragic event is about to take place. But with a recording, analysis of the voice's pitch, intensity, amplitude, and tone could produce data that indicates that the speaker is very happy. Adding such data into the predictive model, might result in the user beginning to see ads for romantic tropical vacations, instead of books about coping with grief.

User interactions with digital assistants will also give rise to new predictive models. Before going to sleep, a user might ask a digital assistant to play relaxing music, lower the temperature of the home, and turn off certain lights. With a new predictive model, when the user asks the digital assistant to play relaxing music at night, the digital assistant might recognize the user's "going to sleep sequence," and proceed to lower the temperature of the home and turn off lights automatically.

In addition to the richness of data in a single voice recording, predictive models based on voice interactions with digital assistants are potentially more robust because digital assistants are always "listening." This "listening" largely takes the form of recording the voice interactions between the user and the digital assistant. Terms of service of the most popular digital assistants typically do not indicate the precise moment when recording starts. Some voice-controlled products have been marketed with an increased focus on privacy concerns. Apple's forthcoming HomePod

speaker, for instance, is said to be designed so that no voice data is transmitted from the device until the "wake word" is spoken.

A digital assistant may begin recording and analyzing voice data even when it is not specifically "turned on" by the user. This makes the potential data set about the user much larger, which results in a more robust predictive model. If the digital assistant is always "listening," its owners' statement, "I'm going to take a nap," could trigger the "going to sleep sequence" described above. If voice recordings are used in conjunction with current predictive models, a user's statement, "we're expecting a child," could be used as a very powerful leading indicator of specific future purchases.

Legal analysis in this growing field should distinguish voice-data recordings (and data derived from these recordings) from the text of these recordings. The current legal framework applicable to voice recordings captured by digital assistants and their use in predictive models is very limited. California has enacted a statute governing certain uses of voice recordings collected from connected televisions. *See* CA Bus. & Prof. Code §22948.20. However, the states generally have not regulated the use of voice recordings from digital assistants, and have permitted use of voice data in various predictive models with relatively little restriction.

Each digital assistant has terms of service and privacy policies that their parent companies promulgate (and change from time to time). Users, therefore, should know that voice recordings are captured by digital assistants with their consent. The terms of service for some digital assistants specifically note that voice recordings may be used to improve the digital assistant itself and may be shared with third parties. Thus, voice data is likely to be used in predictive models.

Call centers have been using real-time voice-data analytics systems. Interestingly, as part of these technology packages, certain voice-data analytics systems can detect and scrub personally identifiable information from voice recordings. Digital assistants may use similar technologies to avoid recording and storing regulated content (e.g., health information, financial information, etc.) to avoid becoming subject to privacy regulations. Doing so may expose those recordings for use in various predictive models.

Even if digital assistants only record interactions between the user and the device, the richness of voice data means that predictive models may become finely tuned to each individual user. Every interaction with a digital assistant may help build a unique user profile based on predictive modeling.

As discussed in this article, certain elements of a user's interaction with the digital assistant may include "expressive content," and both the user and the digital assistant may have constitutional protections. If a digital assistant develops a rich user profile based on both "expressive content," and data from other sources, how much of that profile still enjoys constitutional protections? As individuals sacrifice privacy for convenience offered by digital assistants, will their profile will become more akin to a private journal? As the technologies develop, what rights can the individual be said to have given up to the discretionary use of the service provider and third parties?

Voice Data and the Internet of Things

Digital assistants are not the only voice-controlled devices available to consumers. What about voice-controlled devices that may seem innocuous, or might not even be used by the actual purchaser, like an Internet-connected children's toy? Unsurprisingly, there have already been a few well-publicized data security incidents involving voice data from these types of products. Although the products may be relatively niche at present, the issues raised are not and underscore broader risks associated with the use and collection of consumer-voice data.

One security incident involved a line of Internet-connected stuffed-animal toys. The toys had the ability to record and send voice messages between parents (or other adults) and children through a phone-based app. Voice data from both parents and children was collected and stored on a hosted service. Unfortunately for users, the voice-recording database was publicly accessible and not password protected. Over two million voice recordings were exposed. Worse still, third parties gained unauthorized access to the voice data and leveraged it for ransom demands. Over 800,000 user account records were compromised.

Another recent incident involved a doll offering interactive "conversations" with users. Voice data was transferred to a third-party data processor, who reserved the right to share data with additional third parties. When this toy was paired with an accompanying smartphone app, voice data could be accessed even without physical access to the toy. Security researchers discovered paths to use an unsecured Bluetooth device embedded in the toy to listen to—and speak with—the user through the doll.

Concerns over this doll and other similar products have triggered responses from European governmental agencies. For example, in December 2016, the Norwegian Consumer Council published a white paper analyzing the end-user terms and technical security features of several voice-controlled toys. Forbrukerrådet, #Toyfail: An analysis of consumer and privacy issues in three internet-connected toys (Dec. 2016). Complaints have also been filed with privacy watchdog agencies in several European Union member states, including France, the Netherlands, Belgium, and Ireland. Some complain that voice data is collected and processed by third parties in non-EU states, like the United States, who are not subject to EU privacy and use regulations. Third parties include voice-data processors who also perform voice-matching services for law-enforcement agencies.

More recently, German regulators announced that the sale or *ownership* of one such toy was illegal under German privacy laws after the toy was classified as a "hidden espionage device." Although German regulators are not pursuing penalties against owners, they have instructed parents to physically destroy the toy's recording capabilities. This unusual step may ultimately signal increased regulation of voice controlled consumer products under German law.

Complaints regarding similar products have also been filed in the United States

with the Federal Trade Commission and other bodies. Privacy groups have questioned whether these devices comply with the consent requirements of the Children's Online Privacy Protection Act (COPPA) and its associated rules and regulations. COPPA applies to operators of online sites and services involved in collecting personal information from children under 13 years of age and provides additional protections that may be applicable to voice-controlled toys.

Aside from COPPA, given the lack of comprehensive legislation or regulation at the federal level, there remains a patchwork of state and federal laws that may regulate voice-controlled products. One bill that covers voice data (as part of a broad class of personal information) has passed the Illinois State Senate and is now pending in the Illinois State House. The Right to Know Act, HB 2774, would require operators of websites and online services that collect personally identifiable information to: (i) notify customers of certain information regarding the operators' sharing of personal information, including the types of personal information that may be shared and all categories of third-parties to whom such information may be disclosed; (ii) upon disclosure to a third-party, notify consumers of the categories of personal information that has been shared and the names of all third parties that received the information; and (iii) provide an email or toll-free phone number for consumers to access that information. Importantly, the current draft of the Illinois Right to Know Act also creates a private right of action against operators who violate the act. Whether this bill or similar laws will be enacted remains an open question.

Conclusion

Data collected by voice-controlled digital assistants and other connected devices presents a variety of unresolved legal issues. As voice-controlled features continue to develop, so too will litigation, regulation, and legislation that attempt to balance the rights of users, service providers, and perhaps even the underlying technology itself. The issues presented in this article are deeply interrelated. When even one of the associated legal questions is settled, other issues in this emerging field could quickly follow suit, but new issues will likely emerge.

Eric Boughman is a partner with the Orlando, Florida, corporate law boutique, Forster Boughman & Lefkowitz, where he focuses on legal issues affecting businesses and entrepreneurs.

Sara Beth A.R. Kohut is Counsel at Young Conaway Stargatt & Taylor, LLP, in Wilmington, Delaware, where her practice involves mass tort bankruptcy cases and settlement trusts, as well as privacy and data security matters.

David Sella-Villa is the Assistant General Counsel of the South Carolina Department of Administration assigned to technology, privacy, and information security issues.

Michael V. Silvestro is a Principal in the Chicago office of Skarzynski Black LLC, where his practice focuses on insurance coverage and litigation, including cyber risks. The views and opinions expressed in this article are those of the authors in their respective individual capacities, and do not reflect the opinions, policies, or positions of any of their respective employers or affiliated organizations or agencies.