The Risks of Voice Technology

by Katherine Heires | October 2, 2017 at 6:08 am

These days, voice technology is everywhere. Voice-enabled digital devices and virtual assistants from Amazon, Apple, Google, Microsoft and others can answer a question, provide a weather report, turn up the thermostat or even order a pizza. Businesses are using voice technology to improve call center performance, verify customer account information and assist workers on the job.

Described as “the next paradigm shift in IT” by Gartner Research, voice technology use is booming both at home and in the workplace. “Spoken interfaces are proliferating and successful implementations can reduce operating costs while improving customer experience,” said Dan Miller, lead analyst and founder of Opus Research, an analysis firm focused on intelligent assistance including voice technology.

As of the end of 2016, he estimated, more than 1,200 companies had implemented nearly 2,700 intelligent technology products, 400 of which are voice-enabled, with many more to come. Indeed, according to an IHS Markit report, the AI-powered digital assistance market—which includes voice-enabled devices—is on track to exceed four billion consumer devices by the end of 2017 and will grow to more than seven billion by 2020.

“Voice is finally breaking through as the next interface,” said Peter Cahill, founder and CEO of Voysis, a Dublin-based software firm.

Voice-enabled technology has been around for ages—IBM, for example, has been working on it for decades. But it was the more recent success of virtual assistants like Apple’s Siri and Amazon’s Alexa that really helped put voice technology in the spotlight. Now, the use of voice-enabled technology is becoming increasingly common. Indeed, Gartner Research predicts that 20% of smartphone interactions will occur through intelligent assistants in 2019, and by 2020, a majority of all tech devices will be designed to work with voice control.

“Consumers are becoming increasingly comfortable with the technology, which is driving engagement,” said Martin Utreras, vice president of forecasting at eMarketer. “As prices decrease and functionality increases, consumers are finding more reasons to adopt these devices.” Walmart, for example, recently partnered with Google to enable voice-controlled purchasing.

Talking About Risks

While more people are readily introducing these devices into both home and business settings, experts warn of the risks and challenges associated with voice technology. “The addition of voice absolutely increases the risk level for technology users,” said Nathan Wenzler, chief security strategist at AsTech

Consulting, a cyberrisk management firm. “When you add more features to a device, you are also adding complexity and more code and, as a result, you are introducing more avenues for people to hack into the device. It’s a major risk component.”

> “The minute you have microphones in people’s offices, you are creating a situation where other people will want to listen in.”

Most devices that employ voice-response technology are internet of things devices and, like many data-collecting devices in this nascent category, manufacturers often do not embed adequate security measures into them. “It can be very easy to break into voice-enabled IoT devices and compromise them, and that opens up a lot of problems,” he said.

One such concern is the vulnerability of any device that uses voice as a biometric identification factor. “I can trick the device into thinking I am you or I can intercept your voice and then use your voice print for other purposes,” Wenzler said. Your voice is essentially a password, but since you cannot change or alter it easily, once compromised, its effectiveness for security disappears.

Just as the quality of voice recognition and verification technology has improved, so has the ability to spoof or mimic someone else’s voice for nefarious purposes, according to Dr. Alexander Rudnicky, professor in the Language Technologies Institute at Carnegie Mellon University’s School of Computer Science. This can result in serious misuse and fraud in the form of “replay attacks,” where a voice is replicated and then replayed to allow access to financial accounts, work facilities or virtual assistants.

Voice-enabled technology also raises serious privacy concerns. “Many voice-enabled technologies have always-on microphones and are listening to pretty much everything you say,” said Matthew D. Green, an assistant professor of computer science at John Hopkins University’s Information Security Institute. Although these devices are usually waiting to hear a “wake word” that activates them to listen and respond to a voice command, there is still a possibility that voice data can be exposed. “This definitely creates a privacy risk in corporate environments where your phone may be activated in error and what you thought was a private conversation is sent to Google in the cloud,” he said.

Should hackers then break into the devices or the cloud systems where the data is stored, they could access these private conversations. “The minute you have microphones in people’s offices, you are creating a situation where other people will want to listen in,” Green said. Businesses with voice data that must be protected from competitors’ prying ears should especially be thinking about these types of risks.

Many companies are sensitive to these concerns and offer customers the option to disable voice data collection or delete such data. “Customers can turn any data capture off, in which case we toss the data,” said Michael Picheny, senior manager at the IBM TJ Watson Research Center, of IBM’s policy. In the case of the Amazon Echo device, customers have the option to go through the Amazon website to delete

the questions they have asked Alexa, though the company advises that doing so may inhibit the quality of service.

Earlier this year, these privacy issues came to light when prosecutors in Arkansas sought voice recordings collected by an Echo device as part of a murder investigation. Amazon initially turned down the request for the data, saying in a statement, “Amazon will not release customer information without a valid and binding legal demand properly served on us. Amazon objects to overbroad or otherwise inappropriate demands as a matter of course.” Amazon eventually released the data when the defendant expressed a willingness to do so, but the case is likely only the first of many such conflicts to come between individuals, providers of voice-enabled technology and the courts over privacy rights.

Addressing the Concerns

Businesses thinking about using or developing voice-enabled capabilities must also be aware of the challenges of data collection. “Voice print collections are no different from other types of personal information that need to be protected,” said Larry Ponemon, chairman and founder of the Ponemon Institute.

> “Voice print collections are no different from other types of personal information that needs to be protected.”

Ideally, encryption methods should be used so that the data cannot be easily accessed by cyber criminals, he said. Global businesses also need to be aware of the increased risk coming with the requirements of the European Union’s General Data Privacy Regulations (GDPR), which go into effect in May 2018 and impose strict rules on business regarding the protection of EU citizens’ personal data, including protection against unauthorized or unlawful processing, data breaches or accidental loss of data.

The new law will impose fines of up to €20 million (about $24 million) or 4% of a firm’s global annual turnover for the preceding year, whichever is greater, for any infractions. The risk for many businesses, Ponemon said, is that their chief privacy officer may be focused on protecting more traditional types of information without thinking about newer types of data that also fall under the regulation, such as voice data.

There are several strategies to counter the risks associated with voice technology. For example, to protect against voice spoofing, speech and biometrics consultant Dr. Judith A. Markowitz recommends that companies implement security systems that use multifactor authentication, rather than relying solely on voice. “If you are using speaker verification but are still unsure about the person’s identity, you can use another biometric as a backup,” she said. Companies should also assess the importance of the data being protected to determine how secure it needs to be. “If it is something that requires high security, then you absolutely want to have two or more types of security in place,” she said.

When it comes to guarding against data breaches and preserving voice data privacy, companies should consider using voice-enabled systems that store the data directly on a device or locally, rather than in the cloud. “You are reducing your overall risk by retaining your audio” as opposed to allowing it to reside in the cloud, said Dr. Homayoon Beigi, president of Recognition Technologies and an adjunct professor at Columbia University. Like any other data, however, it is also important to retain only what is necessary.

> “We shouldn’t stop using this technology just because of some security threats. We should be cognizant of any threats and try the best we can to make these products secure.”

The Voice Privacy Alliance, a nonprofit association of IT risk, cybersecurity and privacy experts, has also issued a set of guiding principles for addressing voice data privacy. The VPA advises entities to clearly and simply state the purpose of the collection of voice data, give consumers a choice regarding the use and sharing of this data, and allow them to opt-out at any point. Informed consent terms should always be written clearly and simply so that consumers understand the collection, use, security, sharing, retention and destruction practices for this data. The group also recommends that firms have accountable personnel overseeing data privacy and include voice data privacy monitoring in their routine governance, risk and compliance, and internal audit programs.

Even with such considerations, some experts remain skeptical that companies can adequately protect voice data. Picheny warned that, while today’s customers usually have the option to delete their voice data, this may not always be the case as the technology becomes ubiquitous. “Will every major provider offer that ability?” he asked. Other experts simply advise against using voice technology in the first place. “Your best bet is not to use these devices or capabilities at all,” Wenzler said. “At least not until we get to a point where the security structure is stronger and services become available that don’t record everything.”

Not everyone is so cautious, however. “We shouldn’t stop using this technology just because of some security threats,” said Damon McCoy, assistant professor of computer science at New York University’s Tandon School of Engineering. “We should be cognizant of any threats and try the best we can to make these products secure.”