PROGRAM MATERIALS
Program #29198
November 13, 2019

Alexa, Can You Be Held Against Me in Court?

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

Presentation Outline & Resource Guide

Alexa, Can You Be Used Against Me in Court?

I. How prevalent are smart speakers / digital assistants?

A. Digital Assistant usage growing exponentially (*source: Tractica*)

1. From 390 million users in 2015 to an estimated 1.831 **billion** by 2021
2. 353% increase in usage from 2015 to 2019

B. Digital Assistant usage increases driven by Smart Speakers (*source: eMarketer*)

1. 76% of Smart Speaker users report increased usage in 2018
2. Versus 38% of non-Smart Speaker users

C. Usage Growing Annually

1. Especially among Millennials (nearly doubled)
2. 2019 usage by generation (source: eMarketer.com)
   - *a) 39.3% of Millennials*
   - *b) 17.2% Gen X*
   - *c) 10.1% Baby boomers*

D. Frequency of usage among owners (*source: Voicebot.ai*)

1. 62.7 % use from 1 to more than 6 times per day
2. 23.2% use at least monthly

E. Type of Usage with Business Implications

1. General Questions – 60%
2. Reminders/To do – 39%
3. Calendar access – 27%

F. Applications growing exponentially

1. 135 Apps in Q1 2016
2. 15,000 Apps by Q2 2017
3. Over 70,000 by 2019

II. How are companies are adapting and using?

A. Routine Employee Usage Examples (CNET)

1. Checking & adding meetings to a calendar
2. Enabling voice communications
3. Reading/sending email & instant messages
4. Making & tracking task & to-do lists
5. Reordering office supplies
6. Checking business analytics & statistics

B. Amazon (Alexa), Google & Microsoft (Cortana) Targeting Business

1. Alexa for Business – Integrations & Applications
2. Cortana Assistant – from meeting status to Azure business analytics
3. Integrations with LinkedIn, Salesforce, AWS, Azure, Slack & much more
4. Fleet tracking
5. Financial reporting integrations
6. Systems & support ticket monitoring
7. Customer support

C. Some Corporate Adoption Examples:

1. McDonald's accepting job applications (The Verge 9/15/2019)
2. Small & Medium size business fast adopters (Business News Daily 12/26/2018)
3. 18.536 companies using Alexa (Enlyft.com 2019)
4. WeWork adopting Alexa for Business (Computer World 12/20/2017)

III. Business Confidentiality, Phishing & Hacking Concerns

A. General Business Confidentiality Concerns

1. Access permissions to sensitive corporate information from calendars & emails to sales and other business analytics
2. Accidental device triggers unintentional recordings
3. Overheard background comments & conversations
4. Potential for nefarious instruction to record business conversations
5. Amazon employees listening to Alexa conversations

B. Nefarious Usage

1. Skills can be malicious as some researchers demonstrated: https://lifehacker.com/your-smart-speakers-skills-might-be-a-huge-privacy-prob-1839257208

   a) *The security researchers actually developed two kinds of apps that both worked similarly—one for eavesdropping, one for phishing. In the former, the app would simply do whatever it is you told it to, but it wouldn't stop recording your voice.*

   b) *In the latter, the app would pretend to accomplish a task, wait a bit, then give you a fake message that your device was updated and you needed to provide your password for the update to complete. Any password you then provided was shuffled off to the developer's servers.*

C. Employee Monitoring

1. Employees could be monitored

   https://www.cnbc.com/2018/12/18/alexa-siri-for-the-office-complaining-at-work-is-getting-riskier.html *a) Digital assistants with artificial intelligence, including Amazon's Alexa, Apple's Siri, Google Assistant and Microsoft Cortana, are in the early days of being inserted into office life.*

b) AI will be able to monitor employees' every word (including for tone and sentiment) and also monitor employees' vital health stats.

c) Backers say the productivity gains will benefit employers and workers who will lead better, lower-stress lives, but there is no regulation to oversee the constant monitoring of employees by AI in the office.

d) "These tools will not just be documenting what we say and what we type, but will be observing our reactions, predicting our next steps and tracking the accuracy of their forecasts, even documenting our moods."

e) Regulation? Professional organizations are discussing standards that can be applied. One example of this is the Institute of Electrical and Electronics Engineers, a global technical professional organization. Its Global Initiative on Ethics of Autonomous and Intelligent Systems seeks to encourage AI developers to prioritize ethical considerations, including how employers collect, store, use and share employee data.

f) Sentiment analysis is a process currently used by companies to scan social media and news sites for mention of a company and determine the extent to which it is positive or negative, said Noah Waisberg, co-founder and CEO of AI software firm Kira Systems. Kira's software is being used in the legal profession for document review that in the past would have consumed the lives of law firm associates. According to Waisberg, it would not be a huge technical leap to have these systems listen in on conversations, phone calls, email and text. The data collected could then be used to analyze morale and determine, for instance, whether a new corporate policy is popular with staff or if a change to the 401(k) plan was well received.

D. Webcam/Artificial intelligence interview

IV. Regulatory & Other Privacy Issues

A. Data Protection & Privacy Regulations

1. GDPR considerations making it into U.S. legal system

2. CCPA effective 1/1/2020

a) Highlights:

(1) Focus on transparency and disclosure

(2) Clear statement required when private data being collected

(3) Big data companies have extra rules (more than 4 million consumers)

B. Biometric laws

https://www.gemalto.com/govt/biometrics/biometric-data#

1. Examples include facial recognition, voice as password, etc.

2. GDPR in the EU gives EU citizens control over their personal data with right to be forgotten. Regulation states that personal data shall be collected for "specified, explicit and legitimate purposes." Citizen rights must be properly protected, and data managed carefully and sensibly.

3. In the U.S., there is no single, comprehensive federal law, but rather a patchwork of federal and state laws that overlap and sometimes contradict. Illinois and California are in the forefront here.

C. BOTS – California Law

1. Concern about deceptive use of BOTS

2. Effective 10/2018 called: Bolstering Online Transparency Act (BOT Act)

3. "It shall be unlawful for any person to use a bot to communicate or interact with another person in California online, with the intent to mislead the other person about its artificial identity for the purpose of knowingly deceiving the person about the content of the communication in order to incentivize a purchase or sale of goods or services in a commercial transaction or to influence a vote in an election. A person using a bot shall not be liable under this section if the person discloses that it is a bot."

4. Service providers exempted if they clearly and conspicuously disclose the BOT's identity—if done so, they will not be liable for misleading the other user.

D. Privacy Concerns Are Real

1. A woman in Portland, Oregon found out that her family's home digital assistant, Amazon's Alexa, had recorded a conversation between her and her husband without their knowledge or permission, and sent the audio recording to a random person on their contacts list.

https://qz.com/1288743/amazon-alexa-echo-spying-on-users-raises-a-data-privacy-problem/

V. Caselaw & Digital Assistants

A. Alexa's recordings usage in criminal cases

1. An Arkansas man was arrested in 2016 as a suspect in a first-degree murder case; his Amazon Echo information & recordings were used. https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html

2. A New Hampshire judge ordered Amazon to turn over two days of Amazon Echo recordings in a double murder case. Prosecutors believe that recordings from an Amazon Echo in a Farmington home where two women were murdered in January 2017 may yield clues to their killer. Although police seized the Echo when they secured the crime scene, any recordings are stored on Amazon servers.

https://techcrunch.com/2018/11/14/amazon-echo-recordings-judge-murder-case/

B. Social Media decisions & case law should carry over, as much of the same privacy and admissibility concerns are similar/the same

1. Compton was arrested and charged with arson and insurance fraud. The pacemaker's data was "one of the key pieces of evidence that allowed us to charge him," Lt. Jimmy Cunningham told a local television station. His attorney last year argued that the use of that data violated his client's Fourth Amendment right to privacy, which protects against unreasonable search and seizure. A judge disagreed, saying information about someone's heart rate "is just not that big a deal." (Trial not yet held.)

https://www.cnet.com/news/alexa-fitbit-apple-watch-pacemaker-can-testify-against-you-in-court/

2. Generally speaking and in most cases, the government does not need a search warrant to get personal information that's already shared voluntarily with somebody else, like a bank or internet provider or utility, according to reporting by the Marshall Project.

VI. Implementation Plans & Recommendations

A. The Smart Phone Déjà vu Moment

1. Smart Speakers & Digital Assistants following a similar adoption process

2. Enterprises can apply the lessons learned from the rise of smart phones

3. Many enterprises initially ignored smart phones, but eventually they realized both the productivity gains such devices enabled as well as the inherent corporate confidentiality & privacy issues. This led to the introduction of policies, practices and data protections to address appropriate use.

B. Adoption Options

1. Ignore the problem, as most companies initially did with the introduction of smart phones (and other technologies before that).

2. Ban smart speakers entirely, but with that comes the inherent problem that such bans are difficult, if not impossible, to enforce.

3. Create formal corporate policies and outline acceptable and non-acceptable usage policies.

C. Path to Adoption

1. Create a formal written policy, which should cover:

a) A formal corporate statement regarding which, if any, smart speakers are acceptable to use in the enterprise.

b) Provide use cases, especially within the context of the normal and routine operations of your business, that provide clear examples to employees of both acceptable and non-acceptable usages.

c) Create a formal training program to ensure that all employees are informed of the new smart speaker usage policies, then follow up with routine refreshers.

d) Routinely track and survey employees regarding their use of smart speakers, including asking for examples of how they use them; use their responses to help further develop corporate policies.

2. Other policy suggestions

a) Even if your organization adopts smart speakers, consider banning them entirely in sensitive areas like trading floors, medical offices and other areas where especially sensitive information may be routinely discussed.

b) Encourage use of privacy options like microphone mute and camera blocks that are built into or available as add-ons to most smart speakers.

3. Keep Abreast of Compliance Solutions

a) In the way that Gmail moved from a consumer application to an enterprise application with the introduction of G-Suite, providers may introduce compliance solutions around smart speakers and digital assistants.

Alexa, Can You Be Used Against Me in Court?

BIA

The eDiscovery Experts

November 13, 2019
1:00 PM EST

Brian Schrader, Esq. &
Barry Schwartz, Esq., CEDS

Our Presenters

Brian Schrader, Esq.
BIA
CEO & Co-Founder

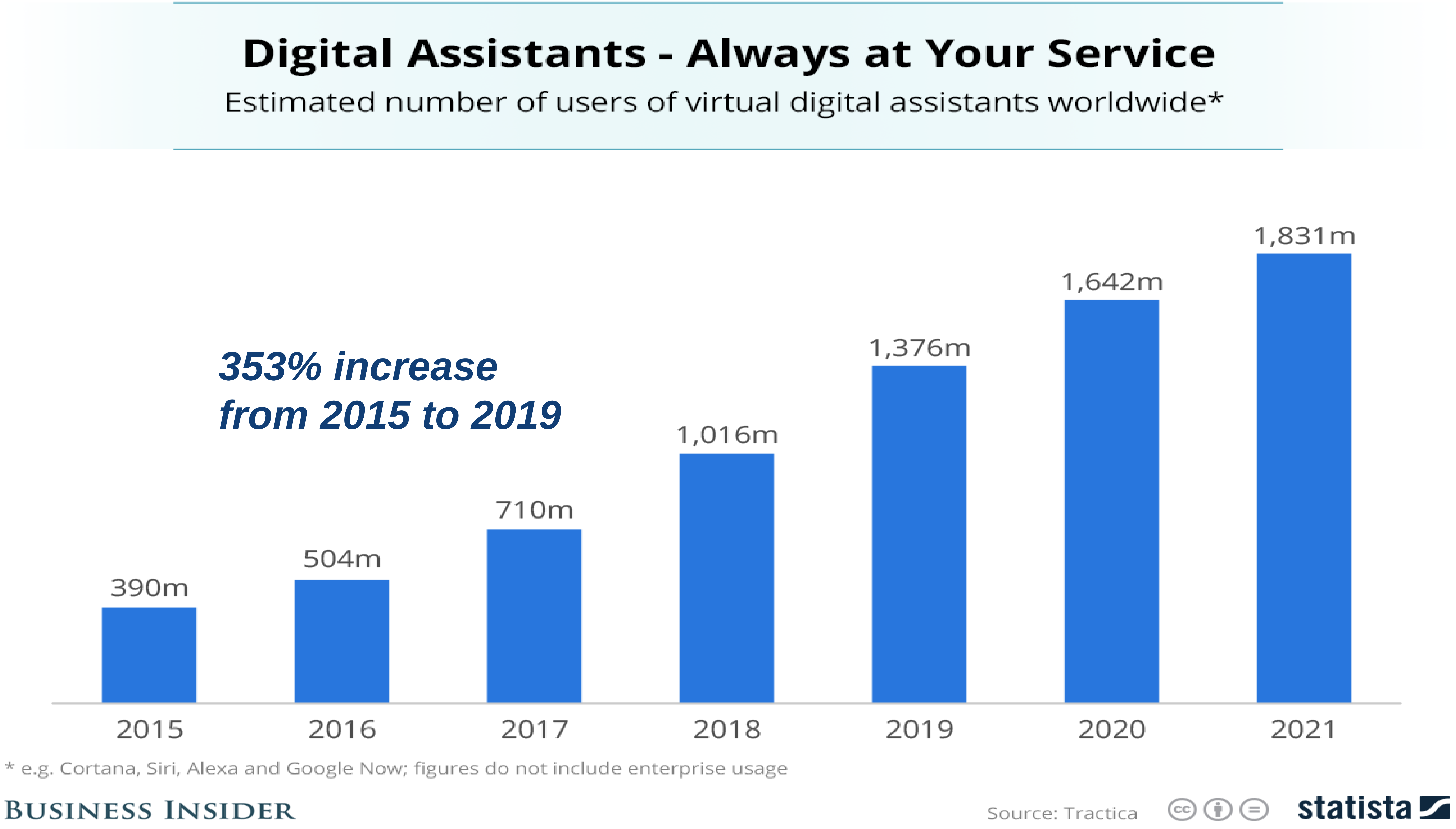
- More than 20 years of experience in eDiscovery, computer forensics, information governance, technology and litigation
- Lectured and participated in numerous panels on eDiscovery, technology and related topics
- Authored articles in *Legaltech News, Law Technology Today* and other publications
- Helped pioneer the industry's first light-touch live data collection tool, DiscoveryBOT, and TotalDiscovery, the first end-to-end enterprise SaaS platform for eDiscovery
- Prior to co-founding BIA, founded several technology companies, and practiced securities and corporate litigation
- Has been engaged in hundreds of high-profile legal matters

Barry Schwartz, Esq., CEDS
BIA
SVP, Advisory Services

- More than 35 years of legal and business consulting management experience
- Highly proficient in electronic discovery and document review matters
- Oversees BIA's advisory division and consults with clients and internal teams to meet specified project goals
- Provides experienced, sound insight in multiple areas, including information management, litigation and discovery, document retention, regulatory compliance and IT security
- Previous experience includes: Senior Staff Attorney of Spriggs & Hollingsworth, Vice President and Business Manager of B-Street Media Corp. and Senior Consultant of AdamsGrayson Corp.

Smart Speaker Prevalence

Just how popular are Digital Assistants?



Digital Assistants - Always at Your Service

Estimated number of users of virtual digital assistants worldwide*

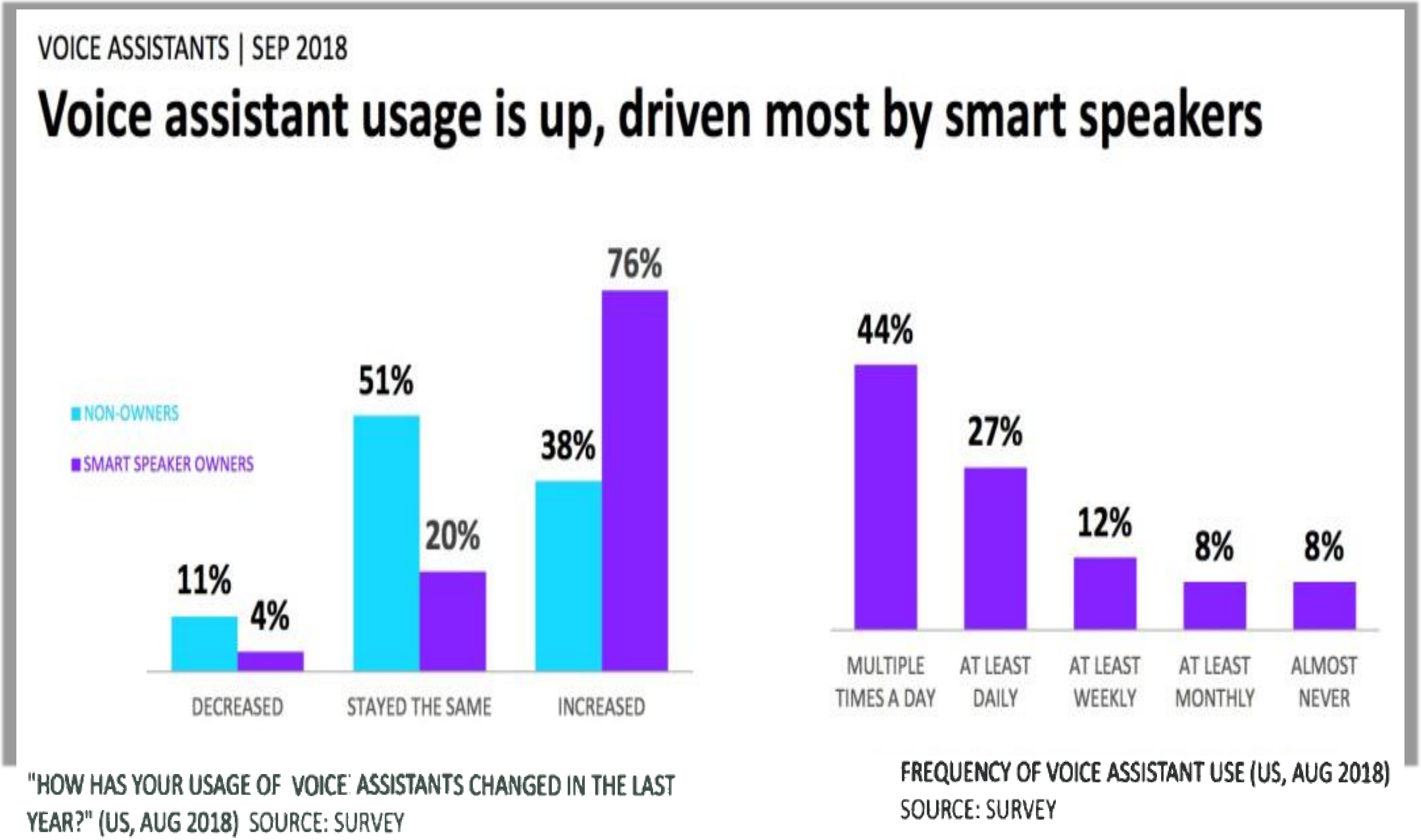
353% increase from 2015 to 2019

* e.g. Cortana, Siri, Alexa and Google Now; figures do not include enterprise usage

Source: Tractica

Smart Speaker Prevalence

How are Smart Speakers driving digital assistant usage?



VOICE ASSISTANTS | SEP 2018

Voice assistant usage is up, driven most by smart speakers

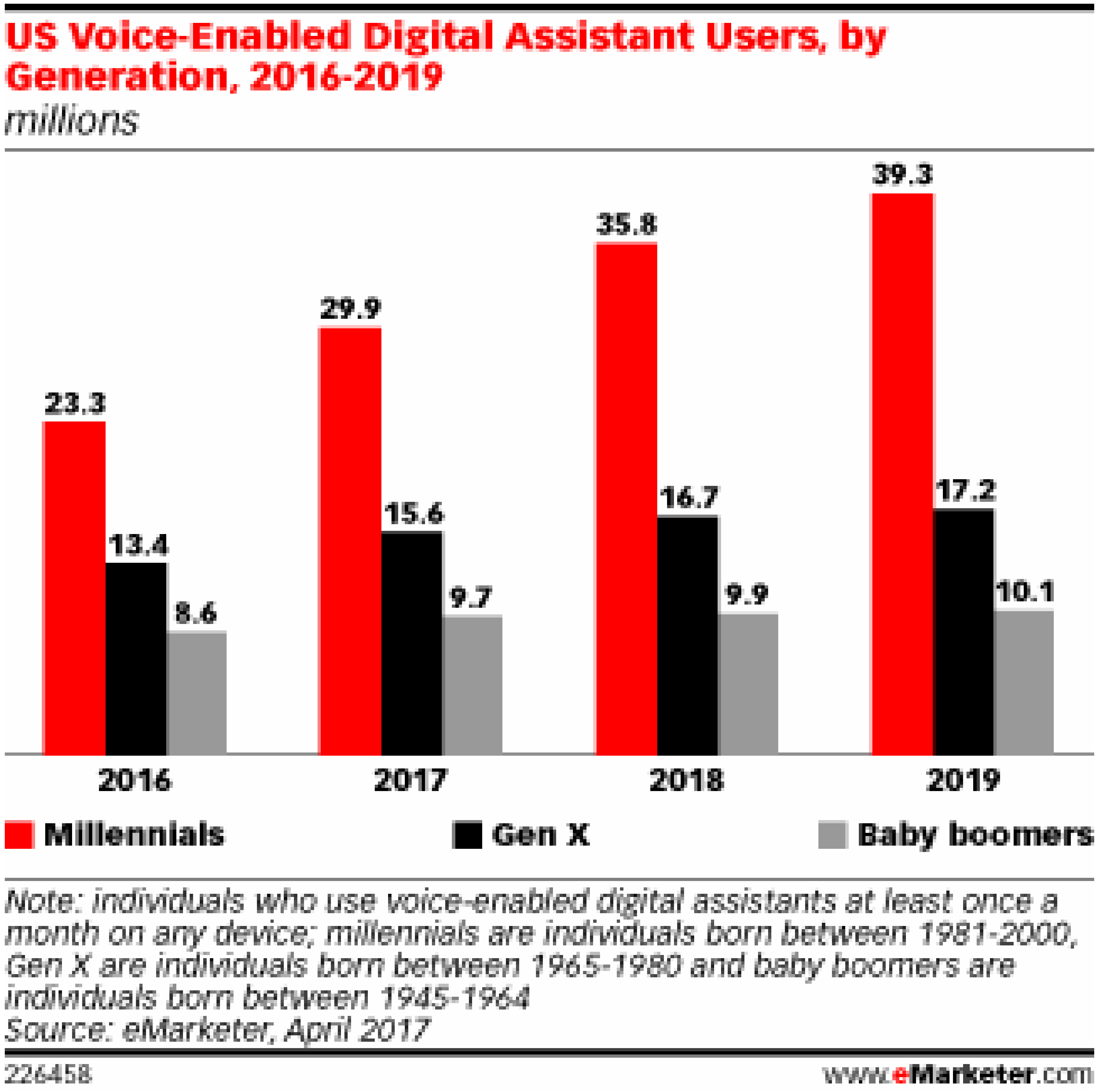
"HOW HAS YOUR USAGE OF VOICE' ASSISTANTS CHANGED IN THE LAST YEAR?" (US, AUG 2018) SOURCE: SURVEY

FREQUENCY OF VOICE ASSISTANT USE (US, AUG 2018)
SOURCE: SURVEY

https://variety.com/2018/digital/news/smart-speaker-adoption-survey-adobe-1202934493/

Smart Speaker Prevalence

Who uses smart speakers?



US Voice-Enabled Digital Assistant Users, by Generation, 2016-2019

millions

Note: individuals who use voice-enabled digital assistants at least once a month on any device; millennials are individuals born between 1981-2000, Gen X are individuals born between 1965-1980 and baby boomers are individuals born between 1945-1964
Source: eMarketer, April 2017

226458 www.eMarketer.com

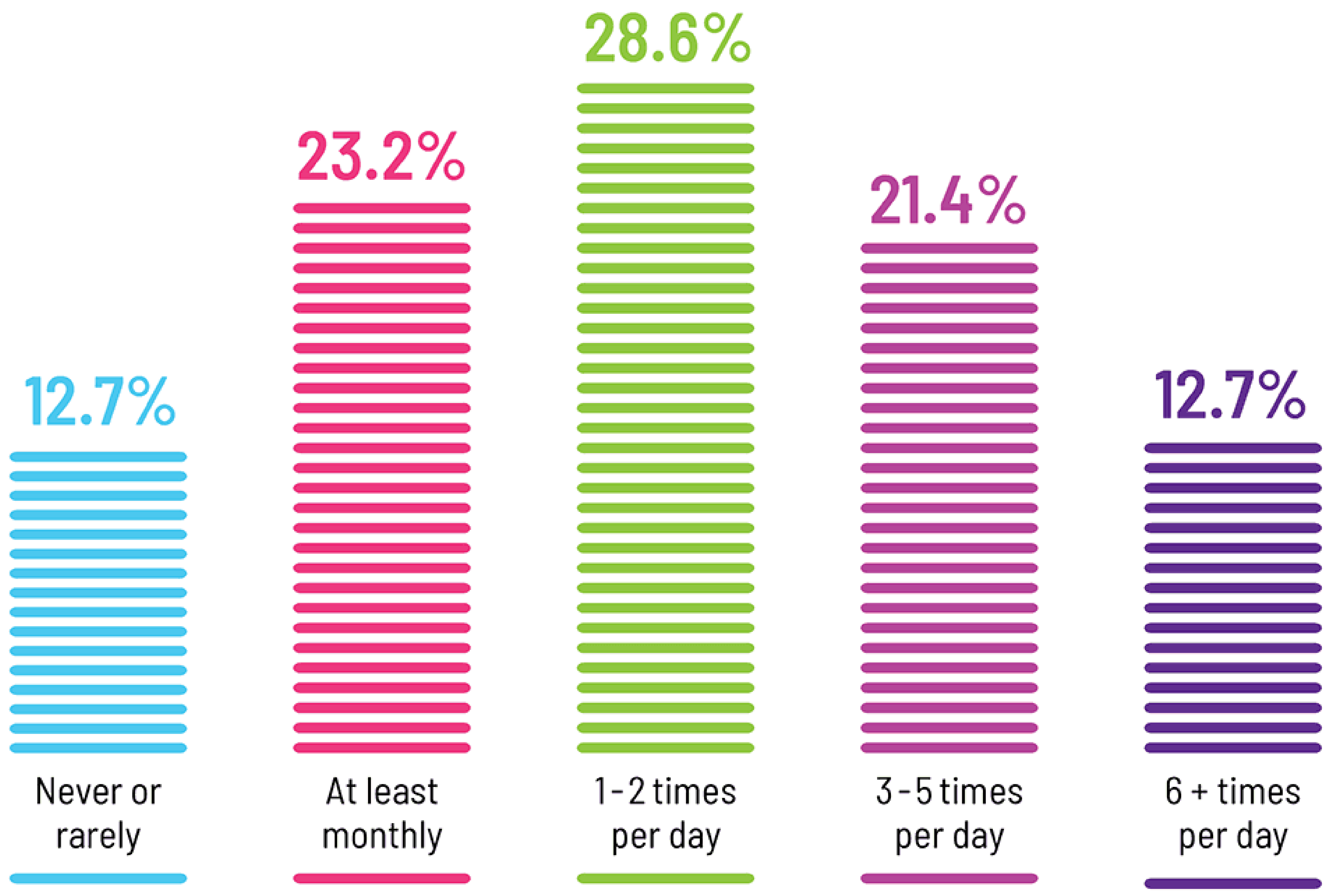
In just four years…

- ***Usage by all groups growing***
- ***Millennial usage nearly doubled***

Smart Speaker owners use their devices:

- ***62.7 % at least once per day***
- ***23.2% use at least monthly***

Frequency of Smart Speaker Use

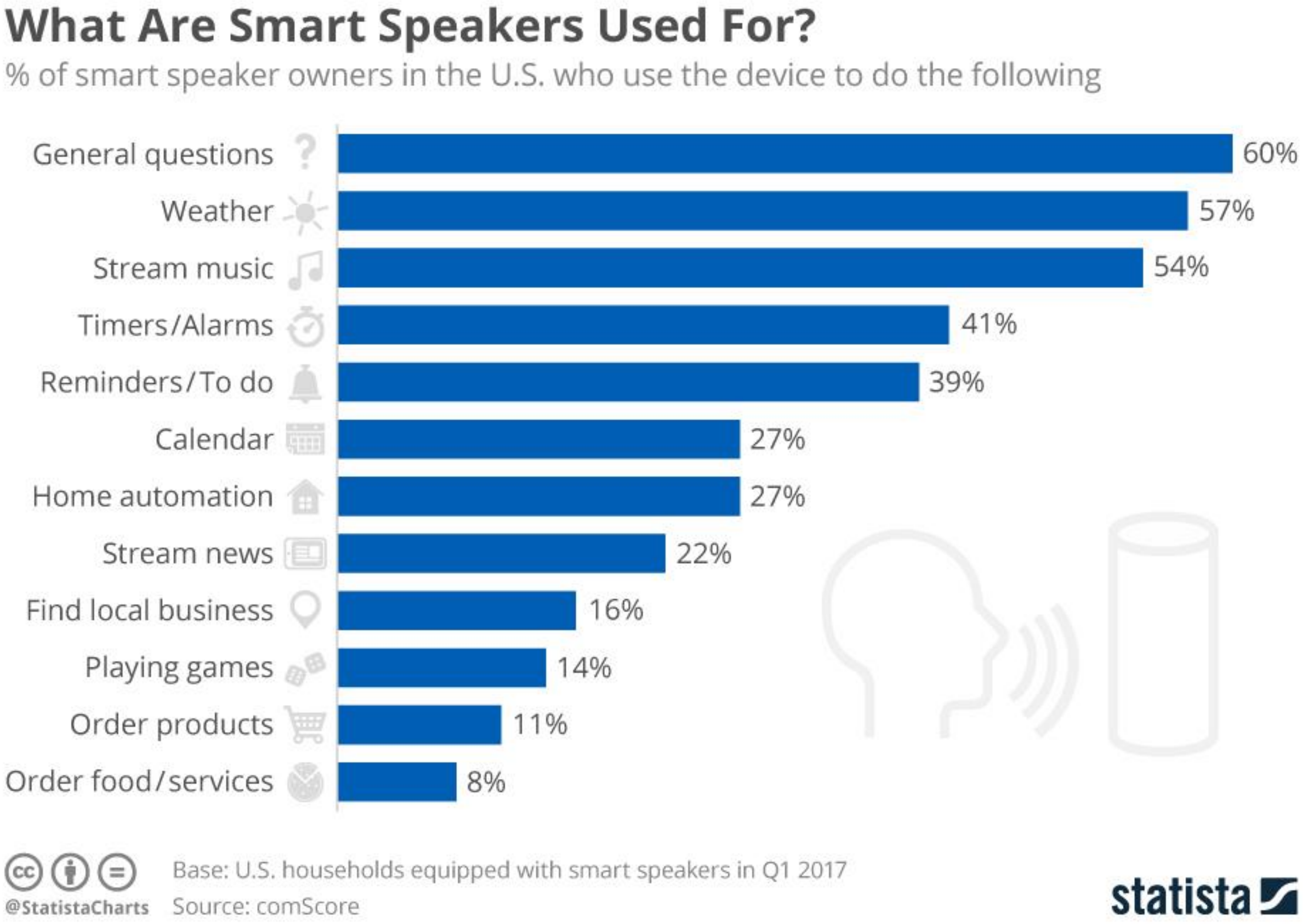


Source: Voicebot Smart Speaker Consumer Adoption Report January 2018

voicebot.ai

Smart Speaker Prevalence

How are Smart Speakers used?



What Are Smart Speakers Used For?

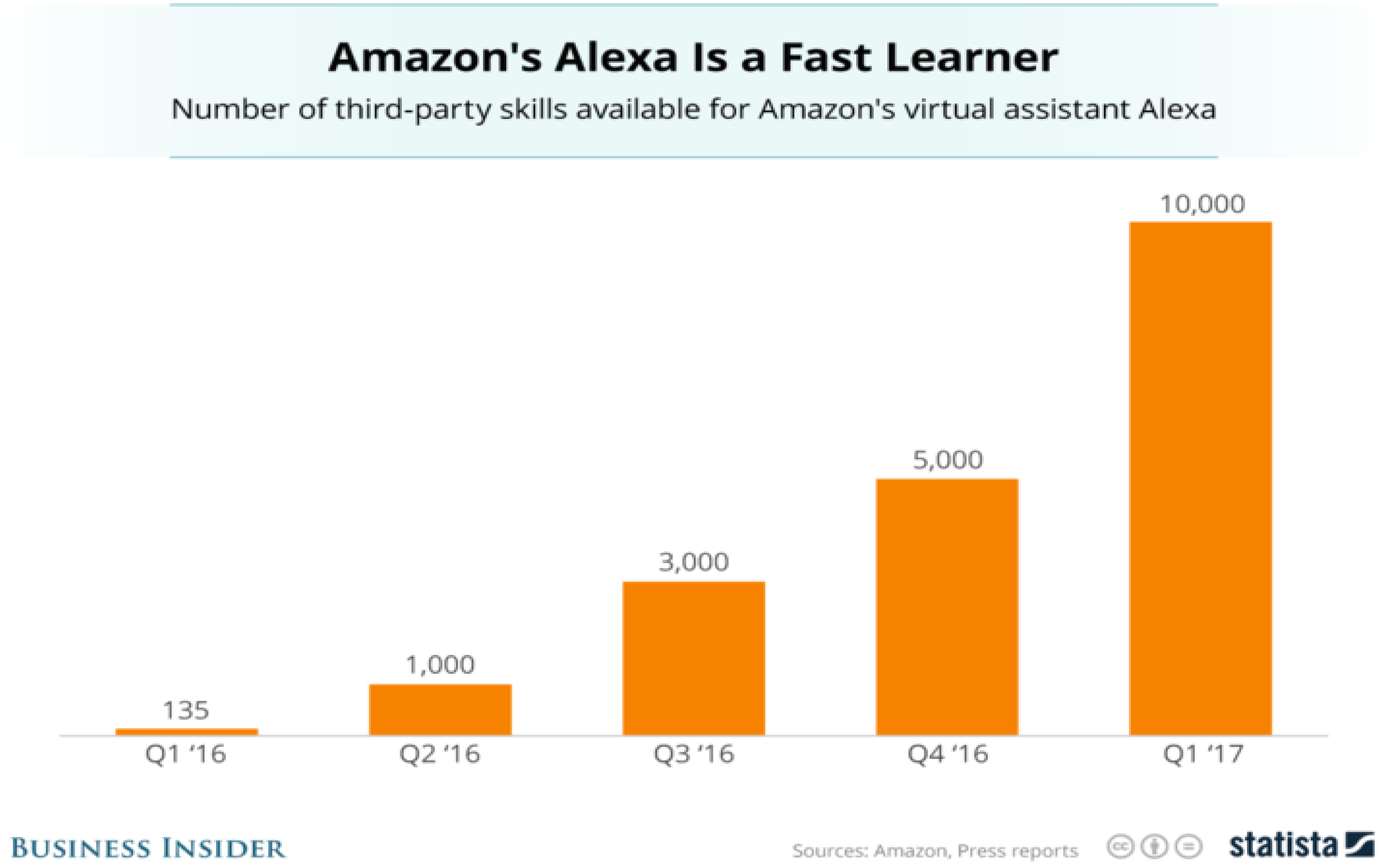
% of smart speaker owners in the U.S. who use the device to do the following

Base: U.S. households equipped with smart speakers in Q1 2017

Source: comScore

Smart Speaker Prevalence

How quickly are new applications being developed?



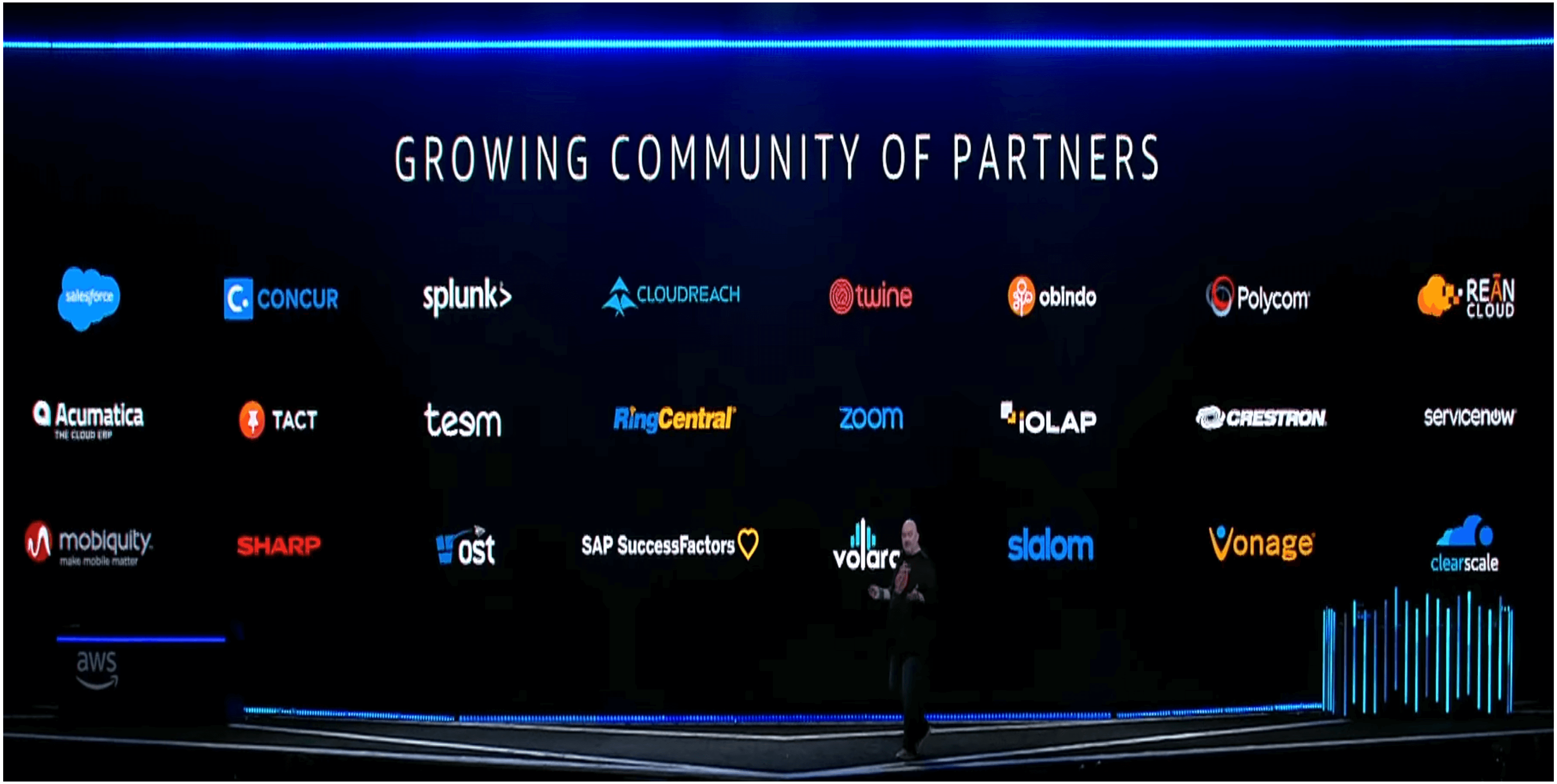
Amazon's Alexa Is a Fast Learner

Number of third-party skills available for Amazon's virtual assistant Alexa

Sources: Amazon, Press reports

Smart Speaker Prevalence

Just a sampling of Enterprise Integrations for Alexa…



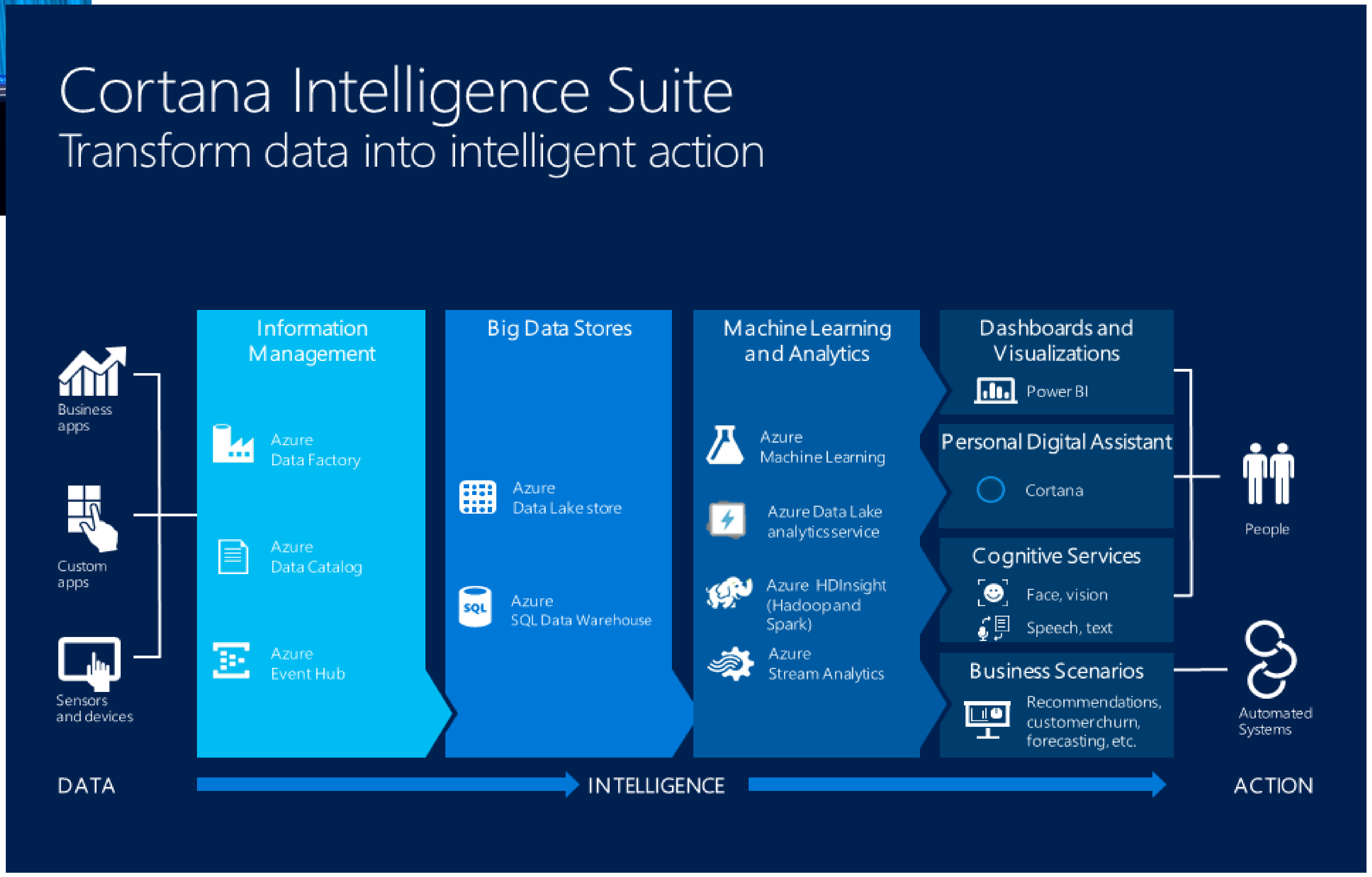
Business Usage of Smart Speakers

How are employees & businesses using Digital Assistants?

NEW!
Alexa for Business
Your intelligent assistant for work
Generally available today

Routine Employee Uses

- ✓ Calendars, Meetings & Scheduling
- ✓ To-Do & Task Lists
- ✓ Voice, Email & Instant Messaging
- ✓ General Knowledge Inquiries
- ✓ Business Intelligence Inquiries


Cortana Intelligence Suite
Transform data into intelligent action

Enterprise & Custom Uses

- ✓ Integration w/LinkedIn, Salesforce AWS, Azure, Slack & much more
- ✓ Fleet Tracking
- ✓ Custom Business Applications
- ✓ Financial Reporting
- ✓ System Monitoring
- ✓ Customer Support

Business Usage of Smart Speakers

Recent headlines regarding Smart Speaker business adoption…

McDonald’s is now accepting job applications through Alexa and Google Assistant

- The Verge 9/15/2019

Alexa for Business: What Small to Medium Businesses Need to Know

- Business News Daily 12/26/2018

18,536 companies use Alexa

- Enlyft.com 2019

How WeWork is looking to use Alexa for Business

- Computer World 12/20/2017

Business Usage of Smart Speakers

Routine business activity & confidentiality concerns

> **Amazon confirms that employees listen to Alexa conversations to help improve digital assistant**
>
> - Geek Wire 04/11/2019

Routine Usages

- ✓ Access permissions to calendars, contacts, instant messages & email
- ✓ Reading/composing emails & instant messages
- ✓ Accessing sensitive business information through integrations

Unintended Usages

- ✓ Unintentional recording of background conversations
- ✓ Accidental triggers result in recording conversations
- ✓ Amazon employee monitoring for general usage improvements

Nefarious Usages

- ✓ Malicious applications
- ✓ Phishing applications
- ✓ Employee monitoring

Smart Speakers & Regulatory/Privacy Issues

Beyond corporate confidentiality issues…

- ✓ Focus on transparency and disclosure
- ✓ Clear statement required when private data being collected
- ✓ Big data companies have extra rules

An Oregon family's encounter with Amazon Alexa exposes the privacy problem of smart home devices

- Quartz 5/25/2018

Smart Speakers & The Courts

Smart speakers already being utilized in court proceedings…

Prosecutors given access to Amazon Echo recordings in first degree murder case.
https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html

Judge orders Amazon to turn over two days of Amazon Echo recordings in double murder case.
https://techcrunch.com/2018/11/14/amazon-echo-recordings-judge-murder-case/

Smart Speakers & The Courts

Key Evidentiary Principle: It's the data that counts, not the medium…

Smart Speakers are just another source of data – and it's the data that counts, not the medium on which it's stored.

Note: Collection of Smart Speaker data can be a challenge

Smart Speaker Adoption & Policies

Does anyone else feel a little déjà vu?

- **Smart Speakers & Digital Assistants are following a similar adoption process.**
- **Enterprises can apply the lessons learned from the rise of smart phones.**
- **Many enterprises initially ignored smart phones, but after realizing not only the productivity gains such devices enabled, but also the inherent corporate confidentiality & privacy issues, they began introducing policies, practices and data protections to address appropriate use.**

Smart Speaker Adoption & Policies

Creating policies & educating employees

Options:

- ✓ Ignore the problem
- ✓ Ban Smart Speakers entirely
- ✓ Create policies & outline acceptable usages

Adoption Path

1. Create a formal policy
2. Train employees
3. Track employee usage

Smart Speaker Policies

Some points to consider…

Policy Considerations

- ***Provide clear guidance & acceptable usage examples.***
- ***Encourage use of privacy options (mute & camera blocks) during sensitive conversations & meetings.***
- ***Ban in especially sensitive areas like trading floors, medical offices, etc.***
- ***Investigate compliance options, like Google did with G-suite; when it focused on corporate usage, compliance options & solutions were introduced.***

Questions?

For more information, please contact:

info@biaprotect.com

Or visit our website:

www.biaprotect.com

Thank you!

BIA

The eDiscovery Experts

This presentation is the property of Business Intelligence Associates and may not be used or reproduced without permission.

Legaltech® news

NOT FOR REPRINT

Click to print or Select '**Print**' in your browser menu to print this document.

Page printed from: *https://www.law.com/legaltechnews/2019/07/10/alexa-can-you-be-used-against-me-in-court/*

Alexa, Can You Be Used Against Me in Court?

It's going to be challenging for any business that has to include such a device in their legal proceedings or regulatory compliance programs. But that won't stop opposing parties from demanding their inclusion.

By **Brian Schrader, BIA** | July 10, 2019

Photo: Zapp2Photo/Shutterstock.com

It hasn't taken long for smart speakers to gain a foothold in modern culture. Though the oldest standalone voice-operated digital assistants have only been on the market for five years, products like Amazon's Alexa and Google Home can now be found in hundreds of millions of households.

Smart speakers are popular for a good reason. With a short voice command you can quickly and easily shop online, get news and weather alerts, control other devices in your house, or say, learn the entire filmography of Bill Pullman, all without booting up your computer or pulling out your smartphone.

The popularity of smart speakers has happened with such speed that it's outpaced the legal issues surrounding them. For businesses that own such a device, or for individual employees who might have a personally owned one on their office desk, the question of who owns any recorded data remains murky, for instance.

It's not our everyday conversations that really are the issue, though. The larger concern is the possibility that a user could accidentally trigger Alexa by saying a word that sounds similar to a command, which then means that entire interaction is recorded and becomes part of the device's history. For instance, Alexa could record a crime as it happens or pick up a conversation where sensitive material like trade secrets are discussed. Those aren't just theoretical either, as such events have already happened.

Targeted at Consumers

In general, devices like Alexa are intended for the consumer market and don't have many features that would make them truly useful tools for businesses. That said, Microsoft recently announced (https://www.youtube.com/watch?v=dXIC2csjxYY) improvements for its Cortana smart speaker that will make it the first device of its type to be targeted at businesses. More will surely follow.

For now, though, the devices are primarily targeted squarely at the consumer marketplace, so using smart speakers in the office may not be very beneficial for most businesses. But such use could carry a certain amount of risk.

First, there's the risk of who might have access to any company data that finds its way into the smart speaker product. One need look no further than the recent news stories concerning humans employed by Amazon to listen to various anonymized Alexa recordings. Simply put, you don't really know who might listen to something Alexa records—intentionally or otherwise.

What's more, user agreements for consumer products generally don't protect such captured data as would be expected in enterprise products. For products targeted at businesses, the company that owns the product nearly always has unequivocal ownership of its data. For consumer devices, there is often less clarity. While saved data is usually still the property of the consumer, the device maker often stipulates that it has the right to access the data for various analysis or other purposes.

Finally, the mere existence of such devices can create unintended consequences and associated costs to the business, like having to include them in any legal, regulatory or other compliance process. Legally speaking, the actual medium where data is stored doesn't make a huge difference. Voice-activated smart speakers may be a new and different way of storing data, but for legal matters, that underlying data recorded by the device likely would be treated the same as paper documents or other kinds of electronic material.

During litigation or discovery, the biggest obstacle would be justifying the collection and analysis of data on a device based on its potential relevance. Any data contained on a company-owned device—even an employee's personal data—is usually discoverable if responsive to valid document requests. Information from personal devices used at a job are also often fair game too—although it would behoove an employer to apprise employees of that policy to avoid surprises down the road. On the other hand, a court likely would set a fairly high bar to justify the discovery of such data from an employee's home device.

A Recurring Problem

If you're feeling a little déjà vu, there's good reason. We've been through all this before—five to 10 years ago, in fact. That's when smartphones and tablets started appearing in the workplace. Back then, companies had the same general options they do now: They can ban their employees from using the devices in question; they can create policies outlining acceptable use; or they can ignore the problem entirely. Unfortunately, many corporations chose the last option, at least initially, and it wouldn't be surprising if many did so again.

Employers who are concerned about the use of voice-activated smart speakers might be best served by clamping down on their general use, at least initially. Certainly, in places where sensitive information is discussed—trading floors at financial institutions, for example—they should be prohibited outright. If you decide to allow the use of smart speakers, make sure you put usage policies and expectations in writing and regularly remind employees what they are, as well as what the ramifications are for disregarding them.

The aforementioned Microsoft Cortana aside, I do find it interesting that smart speakers haven't yet targeted the enterprise market. Devices that eventually do, though, will need to have built-in compliance and discovery functionalities to help companies meet the legal standards and regulations of their respective industries and legal proceedings generally.

Gmail underwent a similar metamorphosis. When Google first introduced the now-ubiquitous email service, it was clearly consumer-focused. However, when Google eventually introduced its cloud-based G-Suite to compete in the business marketplace against Microsoft Office, it included discovery capabilities so that information was saved appropriately and could be extracted if needed. When the next wave of digital assistants comes, we'll likely see enterprise-focused products that contain those kinds of necessary features.

Until then, it's going to be challenging for any business that has to include such a device in their legal proceedings or regulatory compliance programs, as the devices simply haven't been designed to meet such requirements. But that won't stop opposing parties from demanding their inclusion in those processes, just like with smartphones and tablets before them.

New Interactions with Information

To be clear, though, aside from the initial growing pains of any new market segment, there's no reason why digital assistants can't eventually become a standard piece of technology in businesses. Indeed, just like with the smartphone and other such devices, they will likely help increase efficiency and more. After all, they offer an often more efficient and effective way to access and interact with the ever-growing amount of information that we now have available.

When Apple introduced the iPhone in 2007, it changed the world by putting fully usable computers in our pockets. Digital assistants might have a very similar effect. Ten years from now, we could very well look at the technology that will be available to us then and wonder how we existed without it. And with that being the likely outcome, businesses might as well start adapting to the use of these new devices today, so they are ready to take full advantage when that time arrives.

Brian Schrader, Esq., is President & CEO of BIA (www.biaprotect.com (http://www.biaprotect.com)*), a leader in reliable, innovative and cost-effective eDiscovery services. With early career experience in information management, computer technology and the law, Brian co-founded BIA in 2002 and has since developed the firm's reputation as an industry pioneer and a trusted partner for corporations and law firms around the world. He can be reached at bschrader@biaprotect.com* (mailto:bschrader@biaprotect.com)*.*

THE VERGE

GOOGLE \ BUSINESS \ TECH \ 4

McDonald’s is now accepting job applications through Alexa and Google Assistant

Presumably before AI automates the job you’re applying for

By Nick Statt | @nickstatt | Sep 25, 2019, 4:01am EDT

Photo by Budrul Chukrut/SOPA Images/LightRocket via Getty Images

McDonald’s today announced a new initiative the fast food chain is calling the “Apply Thru,” in which owners of Amazon Alexa or Google Assistant devices can begin job applications using standard “Alexa” and “Ok Google” voice commands. The company is envisioning this as a way to give young people more ways to start entry-level careers at one of its restaurants, and that apparently extends to artificial intelligence-powered digital voice assistants.

You can’t actually complete the application process using Alexa or Google Assistant. “After beginning the experience via Alexa or the Google Assistant, all they’ll need to do is answer a few basic questions out loud. They’ll receive a text, following their responses to these questions, with a link to complete the application process online. Simple as that,” reads McDonald’s press release. But perhaps if actually using a computer or your phone to start applying to a job at McDonald’s was too much of a hurdle, getting the ball rolling with a hands-free voice request might do the trick.

The initiative is part of a growing series of tech-adjacent efforts McDonald’s has made over the last few years designed to fashion it as a hip, millennial-friendly brand. The company has struggled over the course of the last decade with the rise of fast casual chains, healthier eating and dieting trends, and shifts in dining culture that have resulted in less late-night drive-thru runs and more mobile app ordering.

MCDONALD’S IS INVESTING HEAVILY IN AI, AUTOMATION, AND ON-DEMAND DELIVERY

In response, McDonald’s has embraced the bold future fusion of AI, automation, and on-demand delivery. It’s also still playing up the nostalgic notion that a McDonald’s gig can be a pleasant, entry-level affair for young people — and not the type of job that seems ripe to be replaced by the very software and robotics advancements the company is betting the future of its business on.

An example of McDonald’s more aggressive tech embrace is its massive partnership with Uber Eats, which includes experimental drone delivery, and now DoorDash, as well as the global rollout of its self-order kiosks. On the other end are marketing gems like the “Snaplications” partnership with Snapchat two years ago and now the Alexa and Google-powered Apply Thru. It’s not clear anyone really wants to apply for a job using an AI voice assistant or the Snapchat app. But McDonald’s figures it can’t hurt.

Meanwhile, the real, tech-infused drivers of its business continue to be its shift to accommodate on-demand delivery and its transition into full-scale automation. McDonald’s is currently testing out even more dramatic steps, like actual robots in the kitchen and voice-activated drive-thru systems. The company has also made a number of acquisitions this year, including an estimated $300 million deal for Israel-based AI startup Dynamic Yield, to bring even more AI advancements and personalization to its drive-thru experience, its various in-store and online menus, and other facets of of the business.

The goal, of course, is to cut costs, keep margins high, and ensure McDonald’s can process, compile, and deliver orders as efficiently as possible all around the world, in both densely packed cities and spread-out suburbs and everything in between. Those sound like exciting problems to work on. But chances are the Apply Thru won’t be accepting applications for those jobs.

lifehacker | Do everything better

PRIVACY

Your Smart Speaker's Skills Might Be a Huge Privacy Problem

David Murphy
10/22/19 2:00PM • Filed to: PRIVACY

11.5K 16 Save

Photo: Shutterstock

Amazon and Google's smart speakers both allow you to supplement them with *extensions* of sorts, the same way you install third-party add-ons to make your web browsing experience even better. Here's the kicker: As with browser add-ons, you're entirely at the mercy of a developer. And should they use their powers for evil, you could be giving up everything you're saying to your device to some random person.

At least, that's the scenario presented by Germany's Security Research Labs (SRLabs), who built a number of dummy Skills (Amazon) and Actions (Google) that passed both company's checks and were actually listed for download to your Echo or Google Home devices. The catch? As Ars Technica describes:

> *"The malicious apps had different names and slightly different ways of working, but they all followed similar flows. A user would say a phrase such as: 'Hey Alexa, ask My Lucky Horoscope to give me the horoscope for Taurus' or 'OK Google, ask My Lucky Horoscope to give me the horoscope for Taurus.' The eavesdropping apps responded with the requested information while the phishing apps gave a fake error message. Then the apps gave the impression they were no longer running when they, in fact, silently waited for the next phase of the attack.*

The security researchers actually developed two kinds of apps—one for eavesdropping, one for phishing—that both worked similarly. In the former, the app would simply do whatever it is you told it to, but it wouldn't stop recording your voice; in the latter, the app would pretend to accomplish a task, wait a bit, then give you a fake message that your device was updated and you needed to provide your password for the update to complete. And any password you then provided was shuffled off to the developer's servers.

Both Amazon and Google have since pulled the offending skills/actions—after being notified of their existence by SRLabs—and are working on extra "mechanisms" and "mitigations" to ensure these kind of exploits don't make their way into other skills and actions. Here are snippets of the statements they provided to Ars Technica:

Amazon:

> *"Customer trust is important to us, and we conduct security reviews as part of the skill certification process. We quickly blocked the skill in question and put mitigations in place to prevent and detect this type of skill behavior and reject or take them down when identified."*

Google:

> *"All Actions on Google are required to follow our developer policies, and we prohibit and remove any Action that violates these policies. We have review processes to detect the type of behavior described in this report, and we removed the Actions that we found from these researchers. We are putting additional mechanisms in place to prevent these issues from occurring in the future."*

Use caution when downloading skills

Here's the thing. People will always try to find new ways to steal your data. Amazon and Google are smart, but not infallible. Going forward, you should treat smart speaker skills as if they were as critical as browser extensions, if not more so. That means not installing skills or actions that sound neat, but come from a third-party source or independent developer you've never heard of. And if you absolutely cannot live without a special add-on for your device, at least do your diligence: Has anyone else used that add-on? Do the reviews seem authentic and not spammy? Is the add-on *absolutely necessary for your day-to-day activities*, or just some fun quirky thing that you'll use a few times and forget about?

And when you've installed your smart speaker add-ons, make sure you're checking your device to see if it remains on—and recording—once the add-on finishes whatever you asked it to do. If so, stop it, and uninstall the add-on, because that's not a good practice. Similarly, be wary of when your devices asks you to do things out of the blue, especially when that came shortly after you used a particular skill. I'm no Sherlock, but it's an awfully strange coincidence if your smart speaker suddenly wants you to verify your password, especially if it's never asked you to do that before, right after you use a brand-new add-on you just downloaded. Maybe...don't do that. (And delete the add-on.)

Or don't download at all

I realize it sounds a bit paranoid to say this, but I'd just go ahead and not use any of these extra skills, actions, add-ons, or whatever you want to call them with your smart speaker. These always-on devices—or, at least, devices that have the power to record what you say—open up brand-new methods for exploiting your privacy, and I remain convinced that no add-on, not even some hilarious joke skill or amazing horoscope action, is worth the risk. Your smart speakers are smart enough. Unless you fully trust what you're adding to them, you don't need the extra hassle (or anxiety).

VIEW ORIGINAL ARTICLE

JDSUPRA®

October 11, 2019

First Impressions: California Attorney General Issues Draft CCPA Regulations

The California Attorney General has issued long-awaited draft regulations for the California Consumer Privacy Act (CCPA), which is scheduled to take effect in 2020.

High level takeaways:

- Big emphasis on disclosure and transparency: both format and content of the privacy notices.
- Separation between the privacy notice for "at or before collection of information" and the "website privacy policy."
- Emphasis on reasoning for taking actions (e.g. not deleting per request, etc.).
- Specific instructions on how to respond to requests (Hint: can't wait until day 44 to reply).
- Guidance on timing for response (Hint: time needed to verify does not extend the 45 days).
- Detailed guidance on how to verify the identity of a requesting consumer.
- Expanded requirements for companies collecting information of 4 million or more consumers (Hint: disclose stats on consumer requests and median time it takes to respond).
- Guidance on the methods for exercising the rights.
- Detailed guidance on how to calculate the value of the consumer's information in order to provide a legal financial incentive.
- Detailed guidance re: CCPA-specific training.
- New records retention requirement for consumer request logs.
- Possible to express an opt-out request through browser preferences/user-enabled privacy controls.

Read the full text of the draft regulations. [View source.]