The Privacy Problem with Digital Assistants

A.I. helpers like Alexa and Siri are useful, but they're not smart enough to keep your questions private—at least not yet.

Amazon's Echo Dot is one of several devices that uses Alexa, the company's digital assistant.

Jeff Chiu / AP

KAVEH WADDELL | MAY 24, 2016 | TECHNOLOGY

For the last century, we've imagined a future where we're surrounded by robotic butlers that are classy, smart, and discreet. We wouldn't think twice of asking an embarrassing question of a robo-assistant, or entrusting him/her/it with sensitive information, because the robot's directive would be to serve only its owner.

Already, there are millions of proto-Jarvises running around in pockets, in the form of digital assistants like Apple's Siri, Microsoft's Cortana, Amazon's Alexa, and (soon) Google's search assistant. These virtual helpers use artificial intelligence to parse what users say or type, and return useful information. More recent updates to Siri and Google have taught the assistants to guess at what users want to know before they're asked, chiming in with notifications about a traffic jam at the appropriate time.

But they aren't quite the robot-butlers we had in mind. In the quest to make our digital lives more convenient, tech companies have run up against a familiar dilemma: It's hard to deliver convenience without sacrificing privacy and security.

For now, conversing with digital assistants is largely a one-on-one affair. Invoke Siri and ask for directions or hit up Google Now for the weather, and your query gets sent to headquarters—a giant server farm somewhere—where it's parsed, answered, and returned to your device.

Like nearly everything else on the Internet, your requests will leave a trail of breadcrumbs. Questions directed at Siri and Google's voice search get sent to their respective companies, paired with unique device IDs that aren't connected to specific users. Apple stores Siri requests with device IDs for six months, and then deletes the ID and keeps the audio for another 18 months; Google's retention policy wasn't immediately available.

When saved queries—and often, associated location data—are connected to user accounts, they can paint a very accurate picture of users' habits, travels, and preferences. Often, that's a great thing: Google Now wouldn't be able to return stunningly useful results without

being able to read your email and dip into your search history. Detailed voice-search history also allows companies to learn user's vocal idiosyncrasies and teach them to understand spoken requests better. But the resulting data-portraits are also available to law enforcement officers who come knocking with a subpoena in hand—there are ways to extract a particular iOS device's Siri identifier—and they can be stolen by hackers who gain access to sensitive servers.

It's not too surprising that the questions you lob at Siri are being recorded and stored, at least for a while. We generally expect our search history to be catalogued, and asking a digital assistant to conduct a search for you is just one step removed from doing it yourself. But with its next-generation assistant, Google is promising to bring its know-it-all artificial intelligence platform even to conversations you're having with other people. That means that Google can capture a wealth of new information, and from a setting that feels inherently more private.

Google is releasing new chat platform called Allo this summer, and its flagship feature is a search assistant that's always waiting in the wings for a chance to help. If a friend messages you to ask if you want to check out a bar downtown tonight, Google will hop in to suggest a few good ones. If you receive a photo of an infant, Google will suggest that you reply "awwww" or "cute!" One tap and Google sends one of those canned responses for you.

How convenient! Except, as *Motherboard*'s Jason Koebler pointed out last week, when you really think about it, Allo's marquee feature is the fact that it's listening in to your conversations. So far, that fact seems only to have drawn the ire of the privacy community (including, of course, Edward Snowden)—a far cry from the mass panic set off more

than a decade ago by Gmail ads based on email content.

For the artificial-intelligence component of Allo to work, Google's servers need to be able to listen to your conversations—so Google chose not to protect messages sent on Allo by default with end-to-end encryption, a strong security protocol that only allows a message's sender and recipient to decode the contents of a message.

Allo will, however, come with an "incognito mode" that enables end-to-end encryption and makes message history disappear after a while, à la Snapchat. That mode can be enabled in individual conversations with one tap, but will disable Allo's artificial-intelligence features.

Releasing a new messaging platform without default end-to-end encryption rubs against a recently established norm. WhatsApp, Facebook's incredibly popular chat app, turned on the feature for all billion of its users last month, to great fanfare from the tech community. Apple's iMessages have the feature, too, although users who back up their conversations to iCloud can't take advantage of it. (Google's current chat offering, Hangouts, isn't end-to-end encrypted, either, so Allo wouldn't really be a step backwards for security as much as it's missing a clear step forwards.)

It's clear the company was thinking about security in developing Allo, but it appears that the convenience that the search assistant would bring—and perhaps the commercial imperative of gathering more information from more places about its users—won out. Thai Duong, a Google security engineer, wrote a blog post last week about Allo's "incognito mode," which he helped design. He discussed the importance of end-to-end encryption, and said he wished it was a default feature. But later, a paragraph of that post, where he made his

preference for default end-to-end encryption clear and promised to push for a more permanent incognito mode, disappeared. According to an update he placed at the top of the post, he deleted the section because "it's not cool to publicly discuss or to speculate the intent or future plans for the features of my employer's products, even if it's just my personal opinion." (Duo, a companion to Allo for two-way video conversations, is completely end-to-end encrypted.)

Allo's always-listening assistant is as close as we've gotten yet to our vision of the quiet computer-butler who jumps in only when needed. Instead of toggling back and forth between a conversation with another human and a dialogue with a digital helper, that helper can follow you to your actual conversations.

But for now, assistants aren't quite smart enough to do all the necessary thinking on their own. They need to rely on powerful servers to do their heavy lifting, communicating back and forth every time they try to answer a simple question—and that step is where the privacy issues crop up.

That likely won't always be the case. As handheld devices are stuffed with more and more powerful processors, the prospect of an artificial-intelligence assistant that lives entirely on your phone is coming within reach. Engineers at MIT announced a chip developed expressly for artificial intelligence earlier this year that would enable A.I. to live entirely on your phone.

Local A.I. would allow a digital assistant to perform certain tasks without an Internet connection. And even when the assistant needs the Internet to deliver an answer, a local A.I. chip could do all the necessary natural-language and voice parsing and decoding on the device,

sending only a final question—ideally, in an encrypted and anonymous way—over the web.

Only when artificial intelligence can work its magic without the Internet will the digital assistant lose its tether to a faraway home base—and truly become an unobtrusive and discreet helper.

ABOUT THE AUTHOR

KAVEH WADDELL is a former staff writer at *The Atlantic*.

Twitter Facebook Email