

Terrifyingly Convenient: Synopsis and Analysis

Article:

http://www.slate.com/articles/technology/cover_story/2016/04/alexa_cortana_and_siri_aren_t_novelties_anymore_they_re_our_terrifyingly.html

Summary:

The article, *Alexa, Cortana, and Siri aren't Novelties Anymore, They're Our Terrifyingly Convenient Reality*, discusses the implications of privacy when the lines become blurred between machine and person. The article begins with an anecdote, a couple having a late night conversation about a friend, when Alexa chimes into the conversation because she thinks that one of the people asked for Alexa to tell a joke. Although it was not necessarily a harmful or scary occurrence, it made the writer realize that these virtual assistants are listening to users' every word, which can seem kind of creepy. The article addresses that these virtual assistants are getting smarter and more capable, leading users to becoming more reliant on them to make their lives easier. This is in contrast to how computers and software was used before. Before, to speak to a computer, users would need to know computer language (programming). Now, a computer is programmed to understand "people language", and users don't need to know "computer language" to interact with a device. Companies like Amazon, Facebook, Google, and Apple, all want these devices to be talked to and used like a personal assistant, rather than a machine. Now, instead of mobile phones and web browsers connecting users to information, users literally do not have to lift a finger to get information in this current age of virtual assistants. The article briefly touches on the implied sexism in the fact that almost all of these virtual assistants have female names, or come with default female voices. The article then highlights a few problems with virtual assistants. The largest problem being that by being a fully voice centered platform, there is less of an open flow of data. The user is only given the virtual assistants preferred search browsers, websites, or apps when users ask a virtual assistant to complete a task, rather than having the choice when users do it manually on a computer or phone. The article ends by speaking to the future of voice activated assistants, suggesting that the best way to create a completely functional assistant is to work vertically: create many virtual assistants that are

incredibly specialized in one task, and once that is complete, work on integrating all of these systems into one mega-assistant that can do everything.

Synopsis:

In an age where software products are intimately connected with your everyday life, that leads to huge implications and concerns over privacy, transparency, and trust. I was reading in a book Swipe to Unlock, about the ethics behind Google's and Facebook's targeted ads. The author felt that they were warranted since Facebook and Google's products are free for the public to use. As a result, their main form of revenue comes from user interaction on ads. The motto that was given in Swipe to Unlock was that "if you aren't paying for your product, then you *are* your product", implying that since users don't pay for Facebook and Google, it is ethical for them to use the information you give to them so that they can give you targeted ads to make a profit and continue to give users the service for free. Now this principle differs slightly when it comes to virtual assistants, since virtual assistants aren't free, however; most of these products don't require a subscription service to continue receiving new updates and access features on their virtual assistant. This brings us to the question, is it ok for a company to take your data, if it improves the experience you will have with the product? This answer differs for different users, but I think that it is safe to say that for users of virtual assistants, the answer would be yes. For them, the knowledge that a company might be able to make an extremely robust profile on them and their families is worth the tradeoff for being able to access information and have a virtual assistant complete tasks for you, completely by voice command. Amazon claims that no user data is stored until Alexa hears you say "Hey Alexa", but is there really a way to verify this? Amazon can claim whatever they want to the public, but they 100% could be storing loads and loads of information on you, and only a select group of people at Amazon would even know if this were the case. From a data preservation and optimization standpoint to avoid an insane amount of storage of data, it would make sense that they wouldn't keep your data, but again, there really is not a way for an outsider to know if they are storing our data or not.

From someone who is very involved with technology by studying Computer Science and interning at technology companies, I think that my perspective on technology companies as well as products that "listen in" on your conversations are not too scary, but for others who may be unfamiliar with how technology works or what it is like at these companies, I can understand how the concept of these virtual assistants can be terrifying. For example, I don't know too much about the government, but isn't this the exact thing that Americans say takes the freedom away from citizens in other countries like China and North Korea? Those countries are ones where citizens live in fear that their governments can listen in on the conversations they are having, even the ones they have in their own homes. If America gets to a point where almost everyone has one of these virtual assistants in their home, and the government demands access to the

software that takes in the data of what is being said in users homes, this could have very scary implications for any user of a virtual assistant. For example, these assistants allow you to connect some pretty harmless things up to your virtual assistant of choice such as calendars, photos, or music preferences. But as these technologies advance, users put more trust into these devices by giving them access to their car, home security, and the ability to withdraw money from their bank, all in the name of making the everyday life easier. Now, if a malicious entity were able to get their hands on this data, or if a company had to fork over this information to an external source, that gives users of virtual assistants virtually no privacy or safety. Imagine what your life would look like if you had no control over your home security system or your own bank account! The article didn't talk too much about the extent encryption is used on the software made that built these devices, but double encryption is a thin line to walk. Facebook thought they were being legendary and giving users more power by doubly encrypting WhatsApp messages a few years ago, so that even Facebook wouldn't be able to see your messages, only the sender and the receiver would be able to see it. However, this gave rise to more illegal action and transactions taking place over WhatsApp, since its users knew that their data and conversations were extremely secure. There is a balance that needs to be reached, but I'm not sure what that would look like.

I'll end with something that I think can be especially concerning given America's current political climate. One of the issues addressed in the article is that when a user asks for information (ex: "Alexa, give me the top news stories of today"), Alexa by default picks a news website, and reads you the top stories from their page. Now, what if Amazon and Donald Trump strike some sort of deal (maybe Trump will teach Besos his tax-evading ways, for example) such that Amazon has an incentive to promote Donald Trump as a presidential candidate. Then, the Alexa could be programmed to give only news sites that paint Donald Trump or the Republican party in a good light. And, without knowing, when people ask Alexa for the news of the day, their view of the world can become skewed from the information the Alexa is giving.

This article speaks more broadly to all of the emerging technologies that will no doubt be making their way into everyday people's lives within the next few decades. As a software engineer, it is important to keep your ethics in line, since with virtual assistants and any other technology product, it is very easy to cross the line between being useful to users, and controlling their views/revealing private information about users to the wrong parties. To be an ethical software engineer at a large company, software engineers should either expose companies for any unethical products they are making, or refuse to make the products in question.