Week 3 Discussion

Please read the article below and summarize it in a couple sentences.

<https://www.cnet.com/news/google-ai-tool-lets-outside-apps-get-smart-without-taking-all-your-data/>

Make sure to answer the following questions in your discussion:

1. Do you trust Google’s claim that the data is not going to be sent to their servers?
2. Would you consider using this tool?
3. How should other technology companies respond to Google’s tool?
4. What’s the difference between this tool and Apple’s process of differential privacy (Also mentioned in the article)

This site is about TensorFlow federated AI software Developed by Google. This software is open source and incorporates federated learning AI system. This software works by collecting data from a lot of devices such as Mobile and tablets teach itself new tricks. This federate is run algorithm right next to your data in devices. This algorithm is already working on our Phones or table to Provide suggestions for email replies on our devices.

TensorFlow federated is already built in some applications like Google Keyboard for android and IOS devices where it suggests message replies for autofill words.

They have mentation in a site that this software helps Google in Google Assistance in the future for engaging in basic conversation.

Google Claim that the data is not going to be sent to their services, but I am not trusting them. The reason is if we check how much Google Assistance has improved in the last few years. But maybe I trust google that this software is just sending ng lessons or sending data anonymously. Because when I switch my phone, my old autosuggestion is removed, and it works like they do not have any data.

This tool is considered until our privacy is protected. This tool is good as far as data has not been sent to Google. But from a developer's perspective, this tool helps developers to create machine learning applications.

I thought that in the current scenario each tech company is constantly competing to stay in the market. Some companies create new alternatives to this tool. But some companies are using this tool to develop their own software for their machine learning applications.

Google allows developers to create applications that run machine learning algorithms next to the data, and it produces some data that is stored in the device and sends some lessons to the developers. Where apple differential privacy is allow developers to create applications that run machine learning algorithms on iOS devices without generating any row data.

Reply

Google has developed a new AI tool that is applied to every of our phone devices without taking our raw data to the cloud. It is supposed to create take only the results of our personal model to analyze it together with other people's models. By doing this, the tool can provide privacy and security of data to the users.

I am not sure if I fully trust Google's claim. I went into the federated learning link (it is a youtube video) in which google said that the cloud analyzed personal results to create global models anonymously. It would be very nice if this was true, but Google's history of being tricky makes me doubt what they say is true. Well, at least they are not taking raw data from us.

If I was a developer I would use this tool. Even if I do not fully trust it, it provides more privacy than the models we had before. Also, as a developer, I think you have to trust what these big companies say. If they end up lying, it is not my job to demonstrate it.

Technology companies are constantly competing. So, if companies don't try to develop alternative technologies that follow the same principle of keeping the privacy of the user, they might fall behind in the market. Because of this, I think that more tech companies will develop more tools like the one in the article.

The difference between TensorFlow Federated and Apple's tool is the next one. Federated learning takes randomized results from models run in our devices to create a global model in the cloud, while Apple's differential learning adds noise to our data to keep it private.

Hello Guillem,

I agree with you I am also not fully trusting Google’s claim. From a developer’s perspective, I would also use this tool. But I think we have to trust Google for this. This tool help developer develops machine learning application. I think so other tech companies are developing more tools like the one in the article but they have to come up with something that this tool is not providing to stay in the competition. nice explanation thanks for sharing.

TensorFlow, an open-source machine learning algorithm, has altered the way mobile applications and machines that run through phones and collect data from phones operate, according to the report. This would encourage people to use their mobile phone activities and enable user behavior on mobile devices. (1). I believe Google's assertion that data is not shared with other servers until the user explicitly grants Google permission to do so and Google is authorized to outsource them.I think that a big brand like Google will share our data because this is private information that is compliant with them and their brand will be at risk if the private information is revealed for these few data shares.

Technology is the term responsible for the world's current changes. In today's world, digital devices are a staple of almost everyone's existence. The amount of data on almost every digital gadget is enormous. Data protection enters the scene to safeguard this information from unauthorized activity. Data protection is a technique used to protect data against hackers, phishing, and other threats. Each and every person values data, thus it is crucial for both businesses and individuals. Therefore, everyone should consider how vital data protection is. Putting in a firewall and antivirus software may lessen the likelihood of data hacking. There should be two alternative approaches to protect data. Physical security and digital security are two possible options.

Hello Nilang,

I Believe in your point that Google not sharing data with other companies but still I doubt that Google is collecting the data from our devices. As a protection view, you true any organization has to use antivirus software and firewall as well as other alternative approaches like digital security.