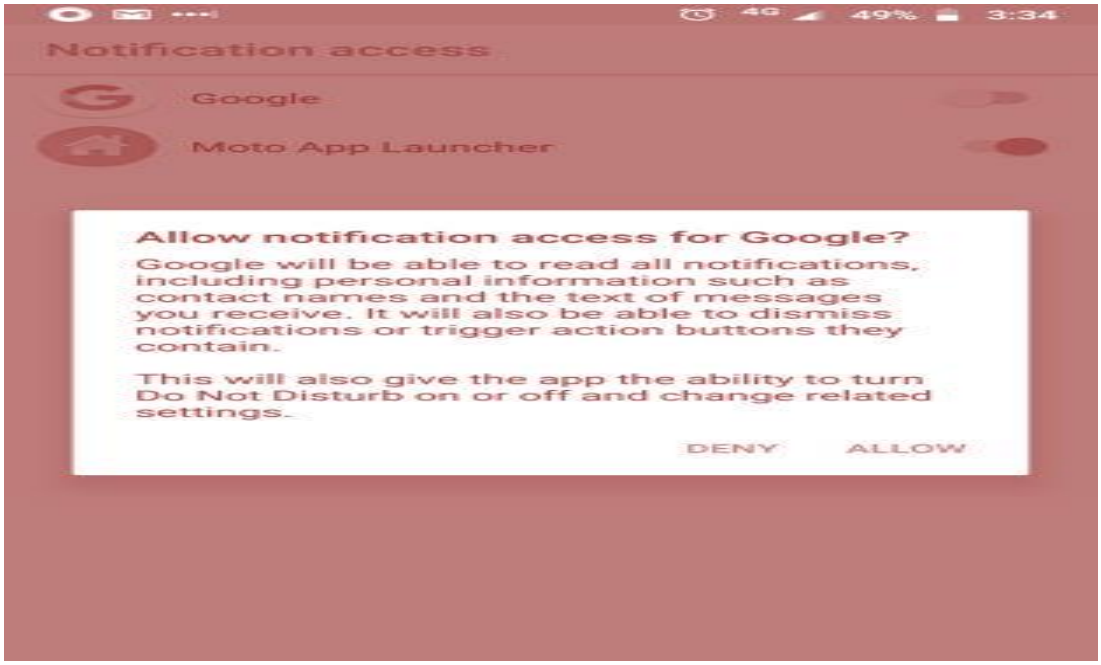
GOOGLE ASSISTANT CAN NOW READ MESSAGES FROM THIRD-PARTY MESSAGING APPS LIKE WHATSAPP

Google Assistant, available on Android devices, can now read texts on third-party apps, including WhatsApp, and reply to them. By orally instructing the Assistant to "read my messages", a card pops up with the last text messages, and the Assistant reads them aloud and identifies the sender and the app they were sent on. Android Police first reported this development.

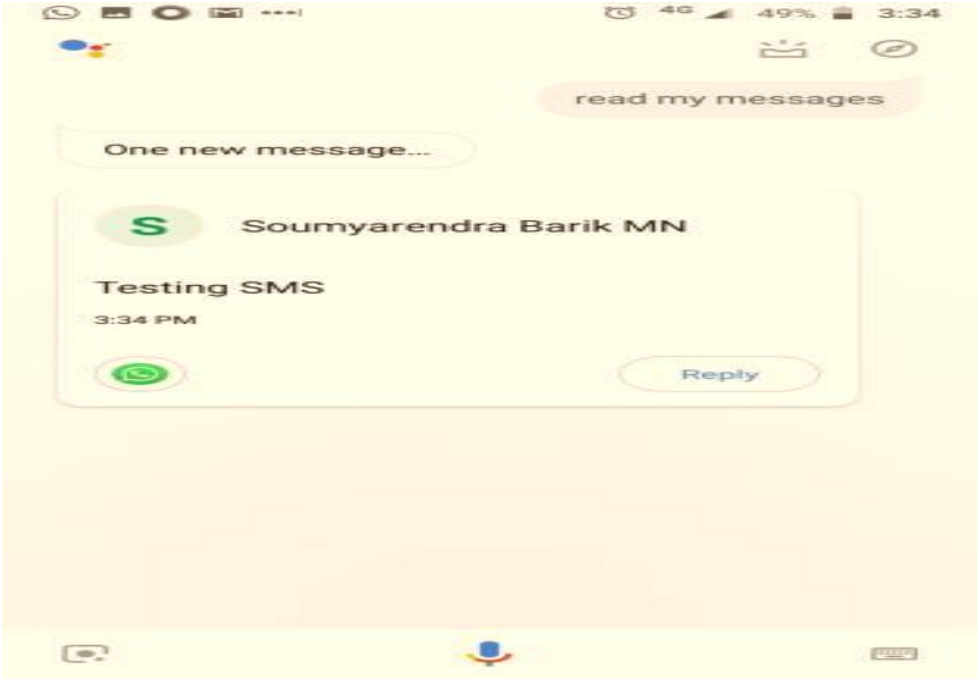
MediaNama has verified that the Assistant could read WhatsApp messages and reply to them if asked to. Android Police confirmed that this feature worked for messages shared on Slack and Telegram as well. Before this, Google Assistant could only read SMS texts and could not access plenty of incoming communication from other third-party apps. We have reached out to Google for comment and will update this story once they reply.

How the feature works

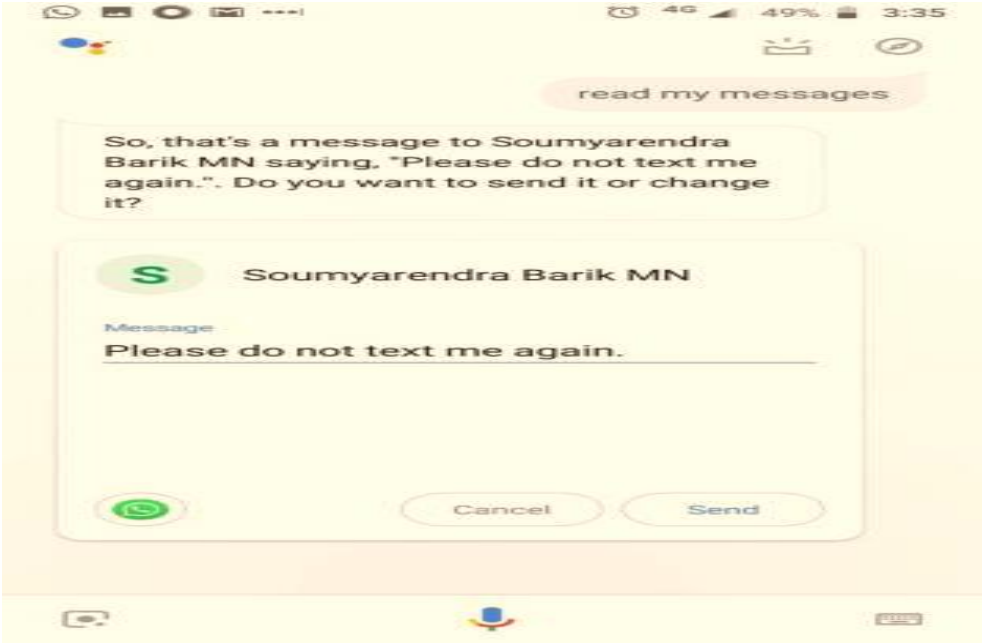
Step 1. To enable the feature, we had to first allow Assistant the permission to read all notifications including contact names and the text of messages.



Step 2. Once we gave the permission, it showed the latest WhatsApp message after we said the phrase "read my messages". This is what Google Assistant said for the following message: "Message from Soumyarendra Barik MN on WhatsApp. Testing SMS."



Step 3. The card that popped up with the message also allowed us to reply to the text then and there, which we could do using our voice. (NB: Please ignore our inter-office banter.)



Source: https://www.medianama.com/2019/08/223-google-assistant-can-now-read-messages-from-third-party-messaging-apps-like-whatsapp/

MESSAGES AND IDENTITY ON WHATSAPP CAN BE MANIPULATED IF HACKED : CHECK POINT RESEARCH

Israeli security company Check Point Research showed that WhatsApp messages and the identity of the sender can be changed if the account is hacked. This was revealed by the researchers during the annual Black Hat security conference held in Las Vegas on August 7. According to the report, a threat actor may potentially:

- Use the 'quote' feature in a group conversation to change the identity of the sender, even if that person is not a member of the group.
- Alter the text of someone else's reply, essentially putting words in their mouth.
- Send a private message to another group participant that is disguised as a public message for all, so when the targeted individual responds, it is visible to everyone in the conversation.

Its worth noting that Check Point had notified WhatsApp about the risks towards the end of 2018 that the risks would allow threat actors to intercept and manipulate messages sent in both private and group conversations, allowing them to create and spread misinformation from channels which appear to be trusted sources. According to the security company, WhatsApp has fixed the third risk but it is still possible to manipulate quoted messages and spread misinformation.

In response to MediaNama's query, a spokerperson of WhatsApp's parent Facebook said, "We carefully reviewed this issue a year ago and it is false to suggest there is vulnerability with the security we provide on WhatsApp. The scenario described here is merely the mobile equivalent of altering replies in an email thread to make it look like something a person didn't write. We need to be mindful that addressing concerns raised by these researchers could make WhatsApp less private – such as storing information about the origin of messages".

Check Point created a tool which allowed the researchers to decrypt WhatsApp communication and manipulate the messages. According to the researchers, by converting WhatsApp's "protobuf2 protocol" algorithm for encryption to "Json", they could see the actual parameters being sent and manipulate them. "By decrypting the WhatsApp communication, we were able to see all the parameters that are actually sent between the mobile version of WhatsApp and the Web version. This enabled us to then manipulate them and start looking for security issues," the report noted.

WhatsApp's encryption debate

This revelation comes at a time when WhatsApp is locking horns with the Indian government over its encryption feature which does not allow the company to read the messages sent through the platform. In order to curb the spread of misinformation, the central government has asked WhatsApp to trace the creator of a fake message. However, WhatsApp declined to concede to the demand because it would require them to compromise with the encryption feature.

However, Dr V. Kamakoti, a computer science professor at IIT Madras in his submission to the Madras High Court mentioned that tracing the originator is possible without breaking encryption. In an interview with MediaNama, Kamakoti had said, "WhatsApp remains the same. Their end-to-end encryption remains the same. There's nothing that we want to change. There's nothing that warrants the change." According to Kamakoti, this can be achieved via: i) consent-based forwarding and ii) Tagging information of the originator along with the message.

- **Consent based forwarding:** According to Kamakoti, a new feature can be added to mark messages as 'forwardable' or 'not forwardable.' "When you are originating a message, you can also be given the option [of making a message forwardable or not forwardable] when I am sending a message to you. I can set that bit and send it to you. That means you cannot forward it to anyone. Now you cut and paste and send it, that still you can do. When you cut and paste; then you become the originator, then you take the responsibility."

- **Tagging originator's information to the message:** "The recommendation is that when a message is generated, originated, you take the message, okay, and at that point, your whole number gets tagged with the message and it travels around with the message. As long as nobody, as long as somebody keeps forwarding the same, the originator information also goes along with it. So anybody who receives the message sees the originator." While speaking about the privacy of the sender, he said that the information about the originator can be encrypted which can be later broken by law enforcement agencies when a message is reported. "If there are privacy and other issues, then it can do an encryption and send that, you know, as a part of the message, wherever in this message. You can encrypt it. Whenever somebody goes to the LEA [law enforcement agency] and says that this message is very disturbing, or derogatory, or whatever, then the LEA can basically talk to WhatsApp and get it [the originator's information, not the message] decrypted," he explained.

Source: https://www.medianama.com/2019/08/223-messages-and-identity-on-whatsapp-can-be-manipulated-if-hacked/

IIT MADRAS'S KAMAKOTI TELLS MEDIANAMA HOW WHATSAPP TRACEABILITY IS POSSIBLE WITHOUT UNDERMINING END – TO - END ENCRYPTION

"WhatsApp remains the same. Their end-to-end encryption remains the same. There's nothing that we want to change. There's nothing that warrants the change."

Dr V. Kamakoti, a computer science professor at IIT Madras, is clear about this. In the last two hearings (on June 27 and July 24) of the case, in which the Madras High Court is deliberating on how the originator of a message on WhatsApp can be traced, Kamakoti's initial submission has heavily featured in the judges' opinion of whether traceability is technically possible. His suggestions on traceability to the Madras High Court, however, had Senior Advocate Kapil Sibal, WhatsApp's counsel in the case, practically palpitating at the last hearing, "If you open up the encryption, there is no platform."

A member of the National Security Advisory Board, which operates under the PMO, Kamakoti became a part of this case when the Chief Secretary of the Tamil Nadu government, Dr Girija Vaidyanathan, at the behest of the court order dated April 25, had convened a meeting between social media companies and law enforcement agencies on May 22. At the last hearing, Justices S. Manikumar and Subramonium directed the professor to make a formal submission (which he did on July 31, available below) and told WhatsApp to respond to it (by August 14).

MediaNama spoke to Dr Kamakoti to understand the submission that he has made and what he thinks of the privacy related concerns:

Dr Kamakoti's submission to the court: Consent-based forwarding and tag the originator

1. Add a tag with the originator's information to the message:

"The recommendation is that when a message is generated, originated, you take the message, and at that point, your whole number gets tagged with the message and it travels around with the message. As long as somebody keeps forwarding the same, the originator information also goes along with it. So anybody who receives the message, sees the originator."

Information need not be stored on the intermediary's server: "[Information of an originator] should be tagged with the message. So that intermediately on your server, you need not store [the originator's information]. This will keep travelling with the message as long as nobody modifies it."

On what constitutes the originator's information: "Every user of WhatsApp will have a unique identity. It *can* be a phone number. It is this ID that we want to capture."

On privacy concerns associated with sharing mobile numbers without consent, especially on WhatsApp groups: "If you are saying that you don't want [me] to forward a message, tell [me] explicitly that don't forward [it]." In that case, "that [forwarding without consent] is a breach of contract between you and me. When you send me a message, and you say it can be forwarded, you don't have any objection to me forwarding it." "So you should have a basic trust with me. You should say you should not forward or you should forward. You should say I should not forward, and I will not forward. If you say I can forward, then I can forward. That's just a breach of privacy between you and me if I forward it without your consent. Then I have to be responsible for it [maintaining that trust]."

2. New WhatsApp feature to classify messages as 'forwardable' or 'not-forwardable':

"Simple" new feature to WhatsApp where "you can have one bit [in the message] that says 'not forwardable', 'forwardable'. One bit." This is how it will work: "When you are originating a message, you can also be given the option [of making a message forwardable or not forwardable] when I am sending a message to you. I can set that bit and send it to you. That means you cannot forward it to anyone. Now you cut and paste and send it, that still you can do. When you cut and paste, then you become the originator, then you take the responsibility."

On whether the originator's information would be visible only to the intermediary (and potentially law enforcement agencies), or to every consumer: "Both ways are possible."

On the possibility of encrypting originator's information to preserve privacy: "There can be issues like privacy and other things. I am a computer scientist. I am not talking about that part. If there are privacy and other issues, then it can do an encryption and send that as a part of the message, wherever in this message. You can encrypt it. Whenever somebody goes to the LEA [law enforcement agency] and says that this message is very disturbing, or derogatory, or whatever, then the LEA can basically talk to WhatsApp and get it [the originator's information, not the message] decrypted."

"So I say 'not forwardable', he should not be able to forward it. That is one part of the story. This is a case where I can see the number as the receiver of the message. I can also get a message in which I can't see the number, but the law enforcement agency, with some due process being followed, [can] go to the court or whatever, can still see the number, the originator's number. That is possible. … I store the number in an encrypted fashion which WhatsApp alone can decrypt, then there's a [something] and there's a due process followed. So these two are the suggestions. This can also be followed."

On the importance of due process and preserving anonymity: "That's okay. See, here you are not violating anything. For example, you can still do this, the originator information in which the anonymity is [maintained]. Anonymity is relieved only in cases of if there is a violation of some rule, that there could be a court order, or there could be LEA, or there could be some due process followed where the originator information can be extracted. And still, I am still telling you, if I

send a message to you, you still know who is the originator. So, even in this solution, even when the originator's information is visible along with the message."

On whether these changes, when implemented at a global level, can be abused by totalitarian regimes: "In a TOTALITARIAN regime, the tagging of originator information with each message, either in encrypted form (decryptable only by Whatsapp) or unencrypted form (viewable by every recipient) is the best in the interest of the user community. It offers very high protection to the users who forward the messages. The reason can be best explained with the following example.

"Let us assume user A originates the message and sends it to B, who in turn forwards it to C, who inturn forwards it to D. Now D finds this objectionable and reports to LEA of that TOTALITARIAN regime. In the current deployment of WhatsApp, where there is no originator information stored, the LEA of the totalitarian regime can find from the message of D that it has come from C, and then by interrogating C find it has come from B and then interrogating B find it has come from A, and interrogating A find the originator is A. Note again we are talking about a TOTALITARIAN regime.

"The biggest problem now comes if inadvertently B has deleted the message after forwarding to C, then the LEA tracing will stop with B. Now B will be subjected to an interrogation of LEA of a totalitarian regime suspecting him to be the originator, which I don't think B will welcome. As WhatsApp claims that it does not store any detail about the messages, B cannot even prove that it came from someone else and he/she just forwarded it and hence not the originator.

"If our suggestion is implemented, that is, In the presence of originator information tagged with each message, either in encrypted or unencrypted form, both B and C are safe and will not be penalized for some information that they have not created."

(Readers, please note, that Kamakoti had not answered our questions about whether these changes, when implemented at a global level, can be abused by totalitarian regimes in the original interview conducted on August 5. MediaNama got this response via email on August 8.)

Dr Kamakoti's views on traceability and defining the originator of the message

On the need for traceability: "[If] somebody receives the bad message, or somebody receives a message that is suspicious, there needs to be a way to [establish] the authenticity of the message. And that is only for the message's receiver. I am getting the message anyway today. Now I have some doubt about that message, or that message is creating some unrest. It can be personal, it can be social, it can be anything. Then I need to have a way by which I know who is the fellow [sic] who has generated [the message]. That's automatic; that's the immediate question."

"Somebody who is not, has not got that message will never know the originator. They will never know that such a message itself has been sent. It is only when somebody goes and complains that this is a derogatory message or some message which is crazy, you know, which is creating some civil disorder, it can be personal, it can be nationwide, it can be anything, whatever it be, something which is not acceptable on social media. At that point only, the LEA comes into the picture. When LEA comes into the picture, if [s/]he's knowing the number, then it's fine, otherwise, if the number is encrypted and stored, then we can do this end-to-end encryption and then I know that only WhatsApp server can find out what it is."

On the intermediary's responsibility: "See, ultimately that is a communication between A and B. So how will a social media intermediary be responsible for it? I don't think WhatsApp can be responsible."

Who is the originator? The protagonist, or the villain, in this whole case — the originator — has thus far remained undefined, both in the court and in the proposed Intermediary Liability Rules. For Kamakoti, "Originator is the creator of the message." This includes three scenarios: first, "you type the message: Hello, Good morning, whatever, MediaNama." Second, "I cut and paste some message and put it and send. … I can now change it," because "when you cut and paste, rather than forwarding it as it is, then you become an originator." Third, "you take an image, you take a media [file] and comment on it, and then forward it, you become the originator."

On taking responsibility for what's shared on social media: Kamakoti likened the need for an originator to the need to know the source of a story in a newspaper. "Every newspaper you take, it is mentioned who is the reporter, who is the editor, who is writing this article that you will read wherever, you have to tell who's writing this article, right? It's news. When it's news, I need to know what is the source. … I don't know whether a newspaper thing that is followed can be extended to social media, I don't know about it. But see, it makes sense for us because suppose I know the actual address, I know the thing, I know a way by which I can find out if this is a genuine message or not. So, that's the pro."

When you modify a message, you become the originator: In "all these three [cases], see these people need to be the originator because all these three essentially mean that I can basically modify the message, and if a message is modified, the original originator who ha[d] sent the message, and which you have cut and paste, that person may not be responsible for this. … If I just get a message, I don't do anything and just forward it, then the originator gets passed on. But if I do any change to it, in these three forms that I have told you, then I become the originator."

On the need to verify the originator: "See, when I receive a message, I should know who is the author, in many cases."

1. To verify potential scams: He gave the example of how on the death of a priest, a fake message was circulated asking for money for his cremation along with bank account details. This message

was immediately followed by another message from the priest's brother-in-law stating that the previous message was a scam. "So two things could have happened, I could have sent the money immediately [and] I would have lost the money. And I could have forwarded it to someone, in which case, I am assisting the crime. I am one of the persons responsible for that crime to spread. On the other hand, suppose I clear this thing that this maybe a fake account, I doubt this, and I don't also forward, if at all a genuine case, then the social cause for which we have such a media is lost. So, in both these scenarios, it will be better if the originator's number is there so that I could call that originator, or I could go to some, you know, some what is this, something is there right? this caller ID. Again, [to find out] who's this. I could call the phone number and find out: 'Is this true? Who are you? What is this?' So, this is one scenario I can give you, but we can have multiple such scenarios. The originator's number if I know, if I as a person who is reading the message, know."

2. Not possible to go to law enforcement agencies on every issue: "Every message I get, it says that somebody needs money. I can't go and ask the law enforcement agencies who is the originator, can I? So I need to know who [it is]. That way everybody is having the good sense. Somebody says that I have a heart surgery, I need money. How will I [confirm] those things today? Right? So that's a pro [of traceability]. So with every message, I have access to the originator information."

3. For a good cause, an originator should have no problem revealing their identity: "I don't know what would be lost if I am doing it for a good social cause. … WhatsApp is a fantastic medium." He mentioned how when a school was devastated by the Gaja cyclone, they were able to contact people as the wi-fi was still working. Mobile towers were affected, but underground cables were still intact. "And within 2 days, we were able to raise a significant amount of money to restructure the school. WhatsApp is doing good stuff like this." "I would have no objection basically in putting my name there [for a good cause]. That is a good cause. So I don't see if there is a good cause, why an originator should not want to reveal his[/her] identity."

On what constitutes the originator's information: "Every user of WhatsApp will have a unique identity. It *can* be a phone number. It is this ID that we want to capture."

Update (August 7, 2019 9:58 pm): The headline of the article was updated. The original headline, "IIT Madras's Kamakoti tells MediaNama how WhatsApp traceability is possible without undermining privacy", was misleading.

Update (August 7, 2019 9:27 pm): This article was updated with the following changes/corrections suggested by Dr Kamakoti for greater clarity and readability:

- *"you need not store" replaced with "you need not store [the originator's information]"*
- *"I can run that bit" replaced with "I can set that bit"*
- *"That we can, that can be both ways." replaced with "Both ways are possible."*
- *"in encrypted FAT [File Allocation Table] which WhatsApp" replaced with "in encrypted fashion which WhatsApp"*

- *"If you are saying that you don't want somebody to forward a message, tell them explicitly that don't forward." replaced with "If you are saying that you don't want [me] to forward a message, tell [me] explicitly that don't forward [it]."*

Source: **https://www.medianama.com/2019/08/223-kamakoti-medianama-whatsapp-traceability-interview/**