The Suno India Show
Pegasus: Understanding the super spy that controls your phone

This is a Suno India production and you're listening to The Suno India Show.

In 2019, lawyers and activists connected with the Bhima Koregaon case began getting calls from researchers of Citizen Lab at University of Toronto. They were told to be careful, their phone was compromised. Now media organisations across the world have come together to expose Pegasus, a spyware developed by NSO Group in Israel. They have found that governments have been using Pegasus to spy on their own journalists, activists and opposition leaders. Amnesty International has been a part of the investigation and its forensic team has confirmed these findings.

Among 300 phones suspected to be infiltrated in India, forty belong to journalists. Other targets include Opposition leaders like Congress MP Rahul Gandhi, virologist Gagandeep Kang, former Election Commissioner of India Ashok Lavasa, poll strategist Prashant Kishor, and an ex-Supreme Court staffer who accused former Chief Justice of India Ranjan Gogoi of sexual harassment. Now after mounting global and national pressure, the NSO has temporarily blocked several of its government clients from using its spyware. In India on the other hand, the Supreme Court will be hearing a plea from senior journalists against the hack.

Hi, this is Suryatapa Mukherjee, your host on this episode of The Suno India Show. I spoke to Anushka Jain, an associate counsel of Surveillance & Transparency at the Internet Freedom Foundation. This is a deep dive on what makes Pegasus special, whether it is accommodated by our laws on surveillance, and how it is affecting Indian citizens.

Host: Can you first tell us what is Pegasus?

Anushka: So, Pegasus is basically an extremely powerful piece of spyware. What I mean by spyware is that, you know, in the old movies like James Bond movies, we see these spies infiltrate enemy organisations and enemy countries, or even just gather information and try to understand what is happening with the other party that you may not have access to through regular means. So, similarly, spyware is a piece of spying software, which allows you to infiltrate the other person's technology devices and gain access to their files, their calls, their text messages, their contacts, and basically their entire life as it is on their phone. And because almost everybody has their entire lives, on their phone, and on their computers, and all those technological devices. And because these devices are all interconnected, to make the experience more smooth. If such spyware is able to infect your devices, that person will hypothetically have access to your entire life, basically. What Pegasus specifically is that it's developed by this Israeli group called NSO. And what it does is, if it infects your phone, it has access to almost everything almost everything on your phone, including SMS, emails, Whatsapp chats, photos, videos, it can activate your microphone, it can activate your camera, it can record your calls, it knows for GPS data, so it can figure out where you are, it has access to your calendar, so you can figure out who you're meeting when you're meeting for how long your

meeting is, it already has access to all your contacts, so it knows who you're talking to.

Host: Could you tell us why everyone is talking about it right now in India and abroad?

Anushka: So in India, we first heard about Pegasus in 2019. When the story broke that Pegasus was able to infiltrate the devices of multiple activists and lawyers who were working on the Bhima Koregaon case, and who were working with oppressed communities. And they were able to do this by exploiting the vulnerability in WhatsApp. So that is when we first heard about it. And you know, there was a lot of hue and cry that was raised at that time as well, but nothing really came out of it. The Standing Committee on IT did a hearing but we never heard about what came out of that hearing. Now, everybody is talking about Pegasus, because The Wire in India and a global media consortium of around 16 News organizations have come together and released this series of reports in which they said that Pegasus has been used to target not just figures in India but across the globe. So politicians, activists, lawyers, journalists, opposition leaders, all across the world have been targeted through the use of Pegasus. And because the Pegasus spyware as I said earlier, it is so problematic. This has become a very big news headline in the recent, in the last two weeks.

Host: What are the special features of Pegasus that sets it apart from other spyware that exists?

Anushka: The special feature of Pegasus basically is that it is so advanced in comparison to other spyware. So for other spyware, for any malware or spyware to be installed in your device, or your cell phone or your computer, there has to be some kind of contact that has to be made, they have to send you a phishing email or a message or you have to click on a link or something like that. With Pegasus, there is zero click infection. So what I mean by zero-click infection is that there are some zero-day vulnerabilities that exist in the operating system of any mobile phone, you know, manufacturer or any app manufacturers system, for example, I can talk about the WhatsApp vulnerability that was there in 2019. So what Pegasus does is it exploits these zero-day vulnerabilities and it can infect your phone without making any kind of contact with you without sending you any messages, without sending you an email and the level of things that it can do once it's on your phone, it can literally control your entire phone. It can make copies of your files, everything that is on your phone is then accessible to it, which is also something that is very advanced. And thirdly, it is extremely difficult to detect that Pegasus is on your phone and that your phone has been infiltrated. These are the three things that make Pegasus so advanced and so problematic.

Host: So, although it is quite technologically advanced, it is not easy to use and access.Could you briefly explain the process of acquiring the spyware?

Anushka: Sure, so, the NSO Group, which has developed Pegasus, says that it works, that their work is only for security purposes and to ensure that people are safe, you know, to enhance the safety of people in general and to help government and intelligence agencies protect their citizens. So, for that, NSO has said that they only sell Pegasus spyware to vetted

governments. And these government contracts are also overseen by the Israeli Ministry of Defence and only when the Israeli Ministry of Defence has given their go ahead is the Pegasus spyware, you know, allowed to be used by the user. So, that is the way in which you can acquire Pegasus. But the one thing that is problematic is that if we don't know how they are vetting these governments, NSO says that they only sell to vetted governments, but there is no transparency with regard to how this vetting process works. How do they decide that this government is okay to send to do they look at human rights records? Do they look at civil rights violations records? Do they look at? Do governments have to tell them who they're going to use them on? And what purpose? So all these all this information we don't know about? So we don't know how they're vetting these countries? And what is the criteria based on which government is marked as vetted? According to NSO, this is a private company making these decisions. Obviously, the Israeli ministry of defense is also involved. But again, we don't know what criteria for the Israel Ministry of Defence, for like, you know, providing approval is. So again, this is a very opaque area when we come to how they are deciding who to send to.

Host: So there has always been some way of spying, whether it is via phone tapping or physically spying on people. Can you paint a picture of how it would affect the life of a person being spied on with Pegasus and what all is possible from the information accessed?

Anushka: So since the Wire has reported that they found pegasus on the phones of journalists, I'm going to use that hypothetical. So if Pegasus is on the phone of a journalist, then they can find out what the journalist is writing about how they are researching it, who they are talking to, for researching, who are their sources, that they will normally not disclose what the source has said, when they are meeting the source, which could also lead to them, you know, finding out the physical location of a source which can be extremely dangerous. And if the government is after that person, they can find out the recordings they can find out, you know, who they're talking to and how they put together their story. If a whistleblower is involved, they can find out the whistleblower's identity. So just imagine that, you know, everything that is on your phone can be accessed by Pegasus. So that's for a journalist. If they have Pegasus on the phone, for example of an opposition leader. They can find out who the opposition leader is talking to what are the next steps, what are this election strategies, what they're going to do, who they're going to talk to, and you know what moves they're going to make to you know, Make sure that like to try to win the next election. So basically you will know what the election strategy is, which is usually highly guarded. And then they can obviously take steps to counter the opposition's election strategy. There's no way to organise protests, because if pegasus is on the phones of people who are higher up who are activists, they will not be able to organise protests, they will not be able to organise rallies, there will be no outcry against the government. And, you know, it will seem like everybody's happy with the government, when they're actually not because they're not able to do anything about it, because the government, because the government is spying on them, they can't take any steps against the government to ensure their own physical safety, as well as the physical safety of other people they know. This would lead us to, you know, basically, leaving behind democracy and ending it. And like, you know, moving towards an authoritarian state where only one party or one group of people have all the power in the country, there's

literally no way to take it away from them, because you cannot strategize how to take it away from them, because they're always listening. And they always know what they are doing against them.

Host: The most crucial part of this whole thing, as you mentioned, is that Israel only sells this to governments. So this could mean the government spying on its own people, although investigation is pending. And now again, and again, we come to this argument of privacy versus national security. So, where do you draw the line between the two or how do you see this issue?

Anushka: See, it is not for me to draw the line between privacy and national security. But then, everything that has to happen in a democratic country has to happen within the bounds of law, you cannot do anything illegal and you cannot do anything outside what the law depicts. That is how our democracy works and we are a democracy. India has surveillance provisions in place, we do have the Indian Telegraph Act, which allows for interception of calls and we have Information Technology Act allows for the interception of data, there's an entire procedure wherein under certain situations, like with security of state or defensive of state, you can make a surveillance request through the authority which can authorise it. And if you get the authorization then you can, you know, do that type of surveillance. So, there is a mechanism in place based on which you can do it. So, if you can justify that for national security, it is imperative that a person's privacy has to be violated, then it has to be proven beyond doubt. That authorization has to be gotten from the authority that is in place according to the current laws in the country. So if they can do that, then obviously you know they can do that type of surveillance. Here I would also like to add that the current surveillance laws in India are also very problematic, it's not like you know, they are perfect. There are multiple challenges against the surveillance laws in India and it has been criticised a lot, because all the power under the surveillance provisions is with the executive and if power is not distributed equally between executive legislature and the judiciary, it is very problematic because then the executive, you know, holds all the power and becomes more powerful than the other two.

Host: IT Minister Ashwini Vaishnaw whose own name has appeared on the Pegasus list, said that any monitoring is done in accordance with law and illegal surveillance is basically not possible in India. What is your take on this?

Anushka: So, what Ashwini Vaishnaw said was that India has a robust surveillance architecture and any surveillance that happens is authorised surveillance and no unauthorised surveillance has taken place. So, in this situation, there are two things that have happened, two paths that we can take. The first path is that the Indian government has acquired Pegasus and then they have gotten authorization requests approved to use Pegasus on Indian citizens. Now, this is problematic because Pegasus is, Pegasus, the use of Pegasus is basically hacking onto somebody's mobile device. And hacking is illegal under the Information Technology Act. As I told you, the only two things that can be done in India with regards to surveillance is that you can intercept calls and you can intercept data. That is when messages are being sent or received, you can intercept those messages and you can find out what is there in the messages. What

Pegasus does is it hacks onto the device and gives you access to the entire device, that type of hacking is illegal in India. So if the government has gotten authorization requests for Pegasus, we have got an authorization request to do something illegal, which obviously is not possible. So, if the use of Pegasus has been authorised, then the government has basically authorised whatever agency carried out these Pegasus attacks to illegally hack Indian citizens. And if that has happened, then obviously we need accountability, we need transparency as to how an illegal act was committed by the government against Indian citizens. That is one. If Ashwini Vaishnaw when he says that no unauthorised surveillance has taken place and by that he means that a Pegasus was not used on Indian citizens by the Indian government, that means that a foreign government has used Pegasus against Indian citizens. Because there is literally no doubt to the veracity of the state of the reports by the Wire and the other 16, you know, media organisations, it has been verified by Amnesty that Pegasus was there. Amnesty's verification process has been vetted by Citizen Lab, which was the first to report about the 2019 Pegasus attack. So there is literally no way that Pegasus was not there. Pegasus was found. It was either done by the Indian government or by a foreign government, if it was done by a foreign government, then in that situation, what is the Indian government doing? Now that we know that a foreign government targeted Indian citizens, it is the duty of the Indian government to protect Indian citizens and their right to privacy and their other rights. So, even after we found that, you know, Pegasus was there on these devices, what has the Indian government done to investigate to find out what is happening and to ensure that they are protecting Indian citizens?

Host: I read something very interesting that Pegasus is not allowed to infect american phone numbers and if an infected phone even travels to the United States, the spyware in the phone self-destructs. So can you venture a guess why Americans are protected from this spyware?

Anushka: This is something that I also found out about recently, and I also, I also raised this question to an expert at dinner on the surveillance architecture in the entire world, not just in India. And they also did not know about this feature of Pegasus. So I think what we can understand from this is that this type of spyware, we still don't know a lot about it. There's still so much to find the founder or find out about how it works, and you know, what these authorizations are. So that is a transparency issue when it comes to spyware and you know something that we need to account for that we still don't know about everything to know about Pegasus, there are still a lot of things that are there that could potentially be more dangerous, that we don't know about. But coming back to your question, I think there might be multiple reasons why this is there. I think the first and most important reason is that because of US and Israel relations, this may be this may have been done. The US has been a strong supporter of Israel on Israel versus Palestine issue for years now. And they probably don't want to, you know, in any way in any way harm their relationships with the United States. Also, it has to be taken into account that the United States military is the most powerful in the world. And if they think that, and because NSO is categorised as a weapon basically, if they think that this is, not NSO sorry, Pegasus is categorised as a weapon basically. If they think that this weapon has been used against their country, they could see this as an attack on their country. And they don't want you know to be in a state of conflict or in a state of war basically, with the United States, because they are their most important supporters. So I think that is what, that may be why US citizens are protected

from Pegasus.

Please rate our podcast and leave a comment if you like it. Underreported and underrepresented stories can become mainstream only if it reaches more people so please support us by visiting our contributing page on our website sunoindia.in or follow us on Facebook, Twitter or Instagram.