based PoS installed which accept Debit card, Credit Card and UPI (Unified Payments Interface) payments using scan and pay option.

Data breach in WhatsApp

1155. SHRI DEREK O'BRIEN: Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a)   the number of times there has been data breaches in the last one year through the application WhatsApp, the details thereof;

(b)   the details of the spyware Pegasus hacking data of Indian citizens;

(c)   whether any Indian Government entity was involved in the data breach, the details thereof;

(d)   whether Government has ascertained the number of persons and their identities, who have been affected by the data breach, the details thereof; and

(e)   the initiatives taken by Government to ascertain the cause of the data breach and its impact, the details thereof?

THE MINISTER OF STATE IN THE MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI DHOTRE SANJAY SHAMRAO): (a) and (b) On May 20, 2019 WhatsApp reported an incident to the Indian Computer Emergency Response Team (CERT-In) wherein it mentioned that WhatsApp identified and promptly fixed a vulnerability that could enable an attacker to insert and execute code on mobile devices and that the vulnerability can no longer be exploited to carry out attack.

On September 5, 2019 WhatsApp wrote to CERT-In mentioning update to the security incident reported in May 2019, that while the full extent of this attack may never be known, WhatsApp continues to review the available information. It also mentioned that WhatsApp believes it is likely that personal data within the WhatsApp app of approximately twenty users may have been accessed out of approximately one hundred and twenty one users in India whose devices the attacker attempted to reach.

It has been reported in media in the end of October, 2019 that social media company WhatsApp has filed a legal case against an entity called NSO Group for allegedly launching cyber-attack that exploited video calling system of WhatsApp in order to send malware to the mobile devices of number of WhatsApp users. It has also been reported that NSO

Group has a spyware called "Pegasus" which can steal information from infected mobile devices. WhatsApp mentioned on their website that the impacted users have been informed about this attack.

(c)   There is no information about any Indian Government entity being involved in the data breach.

(d)   As per information available from WhatsApp, approximately 1400 users were impacted by this attack globally and the attackers attempted to reach devices of approximately 121 users in India.

(e)   CERT-In had sought details from WhatsApp regarding the cause of the incident. WhatsApp has responded mentioning that a buffer overflow vulnerability in the WhatsApp software code was exploited in this incident. CERT-In published a vulnerability note regarding vulnerability in WhatsApp on May 17, 2019 advising countermeasures to users.

The Indian Computer Emergency Response Team (CERT-In) is tracking cyber threats affecting users and issuing advisories to users regarding best practices to be followed for protection of information while using social media and securing mobile devices.

Target of electronic manufacturing ecosystem

1156. SHRI R. VAITHILINGAM: Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a)   whether it is a fact that Government has set a target of creating 400 billion US dollar electronic manufacturing ecosystem by 2025;

(b)   if so, the details thereof;

(c)   whether it is also a fact that Government is considering key measures to incentivize exports from India; and

(d)   if so, the details thereof?

THE MINISTER OF STATE IN THE MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI DHOTRE SANJAY SHAMRAO): (a) and (b) The National Policy on Electronics 2019 (NPE 2019) has been notified on 25.02.2019. The vision of NPE 2019 is to position India as a global hub for Electronics System Design and Manufacturing (ESDM) by encouraging and driving capabilities in the country for