

## PARLIAMENTARY QUESTIONS ON TECHNOLOGY RELATED ISSUES-BUDGET SESSION 2020

---

This document covers questions on technology related policy matters raised during the Budget Session 2020 of the Parliament of India. This session was held in two phases from 31 January 2020 to 11 February 2020 and 02 March 2020 to 23 March 2020. We have divided these questions into the following categories-

1. Social media
2. Digital payments
3. Aadhaar
4. Data protection
5. Cyber security
6. E-commerce
7. Emerging tech
8. Miscellaneous

For each topic, we have highlighted the questions raised by different Members of the Parliament (“MPs”) in both the Lok Sabha and Rajya Sabha, and summarized the government’s response to these questions.

**I. QUESTIONS ON SOCIAL MEDIA**
**A. Questions raised in Lok Sabha**

S.No.	Name of the MP	Question raised	Response by the Government
1.	Rajendra Dhedya Gavit, Shiv Sena (“SS”)	Whether the government — <ul style="list-style-type: none"> <li>• is aware of several cases of mob lynching, fake news, objectionable videos appearing on social media and video sharing sites through print and electronic media and if so, steps taken by the government in this regard; and</li> <li>• has coordinated with State Governments and security agencies to curb the menace of fake news and if so, the details therefor.</li> </ul>	<a href="#">Response</a> by the Ministry of Electronics and Information Technology (“MeitY”): <ul style="list-style-type: none"> <li>• There are media reports about social media platforms being misused to spread various cases of mob lynching, fake news and objectionable videos.</li> <li>• The Information Technology Act, 2000 (“IT Act”) and the Information Technology (Intermediary Guidelines) Rules, 2011 (“Intermediaries Guidelines”) has provisions for removal of objectionable content is removed.</li> <li>• MeitY, the Ministry of Home Affairs (“MHA”) and the police coordinate with various social media platforms to prevent the spread of online fake news.</li> <li>• Through its Information Security Education &amp; Awareness (“ISEA”), the MeitY is creating awareness among users about the importance of following ethics while using internet and advising them not to share rumors/fake news</li> <li>• The Ministry of Information and Broadcasting (“MIB”) has set up a dedicated Counter Misinformation Unit (“CMU”) under the Press Information Bureau (“PIB”) as a measure to counter fake news on policies, schemes, etc. notified by the Government of India.</li> <li>• The CMU takes suo-motu cognizance of fake news going viral on social media and on the basis of outside complaints as well.</li> <li>• MHA has created a Twitter Handle “Cyber Dost” to spread awareness on cyber safety and cyber security.</li> <li>• MHA has published a handbook for adolescents/students on cyber safety.</li> </ul>

2.	Pratima Bhoumik, Bharatiya Janta Party (“BJP”)	Whether the government— <ul style="list-style-type: none"> <li>• is planning to amend the Intermediary Guidelines to make social media liable for advertisement and commissioned content on their platform;</li> <li>• has any mechanism to stop/block the Uniform Resource Locator (“URL”) of any website which is spreading any misleading information or unlawful content; and</li> <li>• The details of websites which were blocked by the Government in each of the last three years due to their misleading information or unlawful content.</li> </ul>	<u>Response</u> by MeitY: <ul style="list-style-type: none"> <li>• MeitY is in the process of amending the Intermediaries Guidelines to make social media platforms more responsive and accountable. The amendments are presently being finalized.</li> <li>• Provisions under the IT Act empowers the government to block information from public access under specific conditions.</li> <li>• The number of URLs blocked during 2017, 2018 and 2019 were 1385, 2799 and 3635, respectively.</li> </ul>
3.	Dr. T. Sumathy (a) Thamizhachi Thangapandia, Dravida Munnetra Kazhagam (“DMK”)	Whether— <ul style="list-style-type: none"> <li>• the government has any data on the number of fake social media accounts operating in the country;</li> <li>• the number of fake social media accounts has increased in the last three years; and</li> <li>• these accounts are used to spread fake news and misinformation on social media platforms.</li> </ul>	<u>Response</u> by MeitY: <ul style="list-style-type: none"> <li>• MeitY does not maintain data pertaining to fake social media accounts.</li> <li>• The IT Act and Intermediary Guidelines has provisions for removal of such objectionable online content.</li> <li>• MeitY, MHA and the police coordinate with various social media platforms to prevent the spread of online fake news.</li> <li>• MHA has issued advisories on cybercrime prevention control, incidents on mob lynching in some states fuelled by rumors.</li> <li>• Through its Information Security Education and Awareness (“ISEA”) programme, the MeitY is creating awareness among users about the importance of following ethics while using the internet and advising them not to share rumors/fake news.</li> </ul>
4.	Behanan Benny, Indian National Congress (“INC”)	<ul style="list-style-type: none"> <li>• Whether the government has taken note of increasing usage of digital and social media in election campaign; and</li> </ul>	<u>Response</u> by MeitY: <ul style="list-style-type: none"> <li>• The government actively participated in a committee constituted by Election Commission of India (“ECI”) to address the issue of misuse of digital and social media in election campaigns.</li> </ul>

		<ul style="list-style-type: none"> <li>The share of Facebook and Google in 2019 election campaign in the country in terms of its reach and money involved.</li> </ul>	<ul style="list-style-type: none"> <li>A code of commitment was released in the last general election held in 2019. Both ECI and social media platforms worked as per the code of commitment for speedy removal of any objectionable or unlawful content.</li> </ul>
5.	Dr Subhas Sarkar, BJP	<ul style="list-style-type: none"> <li>Whether TikTok App poses any counter intelligence threat to the country;</li> <li>If so, whether the government has received any intelligence from the US on negative effects of TikTok on India; and</li> <li>If the government is considering banning the TikTok App.</li> </ul>	<p><a href="#">Response</a> by MHA:</p> <ul style="list-style-type: none"> <li>No inputs regarding counter intelligence threat have been come to the notice of the government.</li> <li>No intelligence has been received from the US.</li> <li>There is no proposal of banning the App.</li> </ul>
6.	Anupriya Patel, Apna Dal	<ul style="list-style-type: none"> <li>Whether the government intends to regulate online video streaming service;</li> <li>If so, the manner in which it proposes to regulate such services; and</li> <li>The manner in which the government proposes to protect freedom of expression and limit censorship in regulating these services.</li> </ul>	<p><a href="#">Response</a> by MeitY:</p> <ul style="list-style-type: none"> <li>The government is committed to the freedom of speech and expression and privacy of its citizens as enshrined in the Constitution of India.</li> <li>Online video streaming services providing curated content are expected to follow the applicable content related domestic laws.</li> <li>Online video streaming services as intermediaries for third party content are required to adhere to provisions under the IT Act and the Intermediaries Guidelines.</li> <li>Such platforms are also expected to remove any unlawful content in terms of Article 19 of the Constitution of India as and when brought to their knowledge through a court order or notice by appropriate government or its agency.</li> </ul>
7.	Feroze Varun Gandhi, BJP	<p>Whether the government—</p> <ul style="list-style-type: none"> <li>has formulated any mechanism to regulate online video streaming services;</li> <li>has conducted any consultation with online video streaming service providers such as Netflix, Hotstar, etc. regarding the content regulation; and</li> </ul>	<p><a href="#">Response</a> by MeitY:</p> <ul style="list-style-type: none"> <li>Please see response to question no. 6.</li> <li>MeitY has not conducted any formal consultation with online video streaming service providers such as Netflix, Hotstar etc. regarding content regulation.</li> <li>There is no proposal with MeitY to regulate such online streaming service providers.</li> </ul>

		<ul style="list-style-type: none"> <li>• is planning to bring a self-regulatory mechanism rather than regulations that are enforceable by the government.</li> </ul>	
8.	Rajyavardhan Singh Rathore, BJP  C.R Patil, BJP	Whether— <ul style="list-style-type: none"> <li>• over The Top (“OTT”) channels/web channels are popular now-a-days;</li> <li>• these web channels allow people to upload content through social sharing platform;</li> <li>• the content being showed on OTT/web channels is being monitored by the government or its agency as these channels are broadcasting violence, abuses and vulgar videos; The government intends on regulating OTT video-on-demand (“VOD”) services provided by online platforms such as Netflix, Amazon Prime, Hotstar and others in India on the lines of independent institutions like Press Council of India and News Broadcasters Association;</li> <li>• the ministry has received notice from the Supreme Court to regulate content on such platforms and if so , the action taken by the government so far in this regard; and</li> <li>• Both the MPs sough details of such online platforms which have adopted a self-regulatory code.</li> </ul>	<a href="#">Response</a> by MIB: <ul style="list-style-type: none"> <li>• The IT Act administered by MeitY has provisions relating to online content.</li> <li>• Online video streaming services providing curated content are expected to follow various content related domestic laws.</li> <li>• Such web channels, which are intermediaries under the IT Act, are also required to follow certain due diligence as prescribed in the Intermediaries Guidelines.</li> <li>• An SLP(C) 010937/2019 has been filed before the Hon’ble Supreme Court of India on the issue of regulation of OTT platforms.</li> <li>• The government had called a meeting of OTT platforms and their industry body is in the process of preparing a self-regulatory code.</li> </ul>
9.	Sunil Baburao Mendhe, BJP	<ul style="list-style-type: none"> <li>• Whether the Government has formulated/proposed to formulate any policy to link social media profile of the users with their Aadhaar number; and</li> </ul>	<a href="#">Response</a> by MeitY: <ul style="list-style-type: none"> <li>• There is no proposal with MeitY to link social media profiles of users with their Aadhaar number.</li> <li>• IT Act has provisions to deal with obscenity and pornography.</li> </ul>

	<ul style="list-style-type: none"> <li>The measures taken by the Government to keep a check on the spread of fake news, pornographic and anti-national content on the social media.</li> </ul>	<ul style="list-style-type: none"> <li>Please see response to question no. 3.</li> </ul>
--	--	--

**B. Questions raised in Rajya Sabha**

S.No	Name of the MP	Question raised	Response by the Government
10.	Harnath Singh Yadav, BJP	Whether— <ul style="list-style-type: none"> <li>it is a fact that the country has been witnessing usage of mobile phones and internet for committing crimes which are against the interest of the country; and</li> <li>the government has taken a decision to monitor all social networking sites.</li> </ul>	<a href="#">Response</a> by MeitY: <ul style="list-style-type: none"> <li>With rapid growth of mobile telephony, improvement in connectivity and development of convenient platforms, there are certain miscreants who use mobile phones and internet for committing crimes.</li> <li>MeitY does not monitor content on social networking sites.</li> <li>The government blocks any information generated, transmitted, received, stored or hosted in any computer resource as per the relevant provisions of the IT Act and the IT (Procedure and Safeguards for Blocking for Access of Information for Public) Rules, 2009.</li> </ul>
11.	Vijay Pal Singh Tomar, BJP	Whether— <ul style="list-style-type: none"> <li>the government has noted the increasing misuse of digital and social media, if so, the action being taken in this regard; and</li> <li>any person involved in such anti-social activities has been apprehended, if so, the number of such persons and the details of punishment awarded to them.</li> </ul>	<a href="#">Response</a> by MeitY: <ul style="list-style-type: none"> <li>With proliferation of new technologies like social media, there are some miscreants who are misusing these technologies for nefarious purposes.</li> <li>Please see response to question no. 3.</li> <li>Police and public order are state subjects as per the Constitution of India. Therefore states are primarily responsible for prevention, detection and investigation through their law enforcement machinery (“LEA”). The LEAs take legal action against the cyber-crime offenders as per the provisions of applicable laws.</li> <li>MeitY does not maintain such data.</li> </ul>
12.	B.K. Hariprasad, INC	Whether— <ul style="list-style-type: none"> <li>it is a fact that the use of hateful and divisive language has increased in the past four years;</li> </ul>	<a href="#">Response</a> by MeitY: <ul style="list-style-type: none"> <li>Due to rapid growth of new and convenient platforms, people across the spectrum are resorting to greater use of social media. Therefore,</li> </ul>

		<ul style="list-style-type: none"> <li>the rise in use of social media by politicians has amplified this disturbing trend; and</li> <li>What is the action taken by the government so far to curb such use including action taken for misusing social media.</li> </ul>	<p>attributing any misuse of social media exclusively to usage by the politicians does not pass muster.</p> <ul style="list-style-type: none"> <li>Please see response to question no.11.</li> <li>Wherever situation warrants, under the provision of section 69A of the IT Act, the government blocks unlawful and malicious online content on a variety of grounds given in the IT Act.</li> <li>Under this provision, 1385, 2799 and 3635 URLs were blocked during the years 2017, 2018 and 2019 respectively</li> </ul>
13.	Digvijaya Singh, INC	<p>Whether—</p> <ul style="list-style-type: none"> <li>the MeitY or MHA has ordered investigation against social media sites which are spreading fake news or posting provocative statements through their social media accounts</li> <li>the government has accessed a study conducted by the London School of Economics (“LSE”) on the subject; and</li> <li>the government has taken any action against all those who have been spreading fake news.</li> </ul>	<p><a href="#">Response</a> by MeitY:</p> <ul style="list-style-type: none"> <li>MeitY has not ordered any investigation against social media sites which are spreading fake news.</li> <li>MeitY has not accessed any study by the LSE on this subject.</li> <li>With a borderless cyberspace coupled with the possibility of instant communication and anonymity, the potential for misuse of cyberspace and social media platforms for criminal activities including spreading fake news is a global issue.</li> <li>Please see response to question no. 1.</li> </ul>
14.	Md. Nadimul Haque, All India Trinamool Congress (“AITC”)	<p>Whether the government is planning on issuing a notification or rules to social media intermediaries regarding sharing of data on request from government agencies.</p>	<p><a href="#">Response</a> by MeitY:</p> <ul style="list-style-type: none"> <li>MeitY is in the process of amending the Intermediaries Guidelines to make social media platforms more responsive and accountable. The amendments are presently being finalized.</li> </ul>
15.	Veerendra Kumar, Loktantrik Janata Dal	<ul style="list-style-type: none"> <li>Whether Government has noticed any misappropriation of data in social media platforms, if so, the details thereof and the corrective steps taken by government in this regard; and</li> </ul>	<p><a href="#">Response</a> by MeitY:</p> <ul style="list-style-type: none"> <li>The government intervened in the matter of misappropriation of data and interference by Cambridge Analytica (“CA”) in Indian elections by seeking clarifications from CA and Facebook. The matter has been handed over to CBI for investigation.</li> <li>The proposed Personal Data Protection (“PDP”) Bill, 2019 seeks to bring in a culture of privacy by laying down obligations for data</li> </ul>

		<ul style="list-style-type: none"> <li>The extent to which the personal data protection legislation will be helpful in this regard.</li> </ul>	<p>fiduciaries (like social media platforms). Rights for data principals under the PDP Bill will be enforced by a regulator, namely the Data Protection Authority of India.</p> <ul style="list-style-type: none"> <li>The PDP Bill is expected to address misappropriation and misuse of personal data.</li> </ul>
16.	Amar Patnaik, Biju Janta Dal (“BJD”)	<p>Whether—</p> <ul style="list-style-type: none"> <li>the government is aware of any actions by political parties to utilise WhatsApp groups for campaigning;</li> <li>such usage of social media groups is a risk to control rogue messages; and</li> <li>if so, what are the steps taken by government to mitigate these risks.</li> </ul>	<p><a href="#">Response</a> by MeitY:</p> <ul style="list-style-type: none"> <li>MeitY has no information about actions by parties to utilise WhatsApp groups for campaigning.</li> <li>Please see response to question no. 4</li> <li>WhatsApp has introduced various features in its platform including limiting the forwarding of messages, labelling of forwarded messages as well as ease of reporting abusive messages.</li> </ul>
17.	Derek O Brien, AITC	<ul style="list-style-type: none"> <li>The number of times when Government has blocked access to online resources under section 69A of the IT Act and the rules notified thereunder, in the last three years; and</li> <li>Whether the person or intermediary hosting the content has been sent a notice in each case to submit their reply and clarifications; and if not, the reasons therefor.</li> </ul>	<p><a href="#">Response</a> by MeitY:</p> <ul style="list-style-type: none"> <li>The government passed 10, 18 and 40 blocking orders under section 69A of the IT Act in the last three years i.e. 2017, 2018 and 2019, respectively.</li> <li>The government blocked 1385, 2799, 3635 URLs in the last three years i.e. 2017, 2018 and 2019, respectively.</li> <li>MeitY issues notices to the concerned person or intermediary posting/hosting the URL, wherever possible, to appear or send their response, at least 48 hours prior to the meeting of the committee for examination of request for blocking.</li> </ul>
18.	Shanta Chhetri, AITC	<p>Whether the government —</p> <ul style="list-style-type: none"> <li>has plans for online video content regulation; and</li> <li>is planning to restrict streaming companies, censorship of online video content on shows by implementing new legislation on online streaming of videos.</li> </ul>	<p><a href="#">Response</a> by MIB:</p> <ul style="list-style-type: none"> <li>Please see response to question no. 8.</li> </ul>



## II. QUESTIONS ON DIGITAL PAYMENTS

### A. Questions raised in Lok Sabha

S.No.	Name of the MP	Question raised	Response by the Government
19.	Chandra Sekhar Bellana, Yuvajana Sramika Rythu Congress (“YSR Congress”)  Magunta Sreenivasulu Reddy, YSR Congress	<ul style="list-style-type: none"> <li>The number of Unified Payment Interface (“UPI”) transaction conducted in the country during the last year, month-wise and State/UT-wise;</li> </ul> <p>Whether—</p> <ul style="list-style-type: none"> <li>the government has ensured the safety of such UPI transaction and if so, the details thereof and the steps taken by the Government in this regard; and</li> <li>any grievance platform has been provided by the Government to the user to register their complaint regarding UPI Transactions.</li> </ul>	<p><a href="#">Response</a> by MeitY:</p> <ul style="list-style-type: none"> <li>UPI based digital transactions observed a significant growth over the last few years.</li> <li>State/UT wise transaction details are not maintained.</li> <li>The government adopted various measures to ensure safety of UPI based digital transactions:                             <ul style="list-style-type: none"> <li>The Indian Computer Emergency Response Team (“<b>CERT-In</b>”) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies. 28 such advisories have been issued for users and institutions.</li> <li>RBI has advised authorised entities/banks issuing Pre Paid Instruments (“<b>PPIs</b>”) to carry out special audit by empanelled auditors of the CERT-In.</li> <li>Guidelines for Chief Information Security Officers (“<b>CISO</b>”) regarding their key roles and responsibilities for securing applications/infrastructure and compliance were released by the government.</li> <li>Government has empanelled 90 security auditing organisations to support and audit implementation of information security best practices.</li> <li>Crisis management plan formulated for countering cyberattacks and cyber terrorism for implementation by all Ministries/ Departments of central, state governments and their organizations.</li> </ul> </li> </ul>

			<ul style="list-style-type: none"> <li>○ Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organizations in government and critical sectors.</li> <li>○ 44 drills conducted by CERT-In, where 265 organizations from different states and sectors participated.</li> <li>○ 9 drills were conducted in coordination with RBI and the Institute for Development and Research in Banking Technology for financial sector organizations.</li> <li>○ Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) launched by the government. The centre is providing detection of malicious programs and free tools to remove the same.</li> <li>● Integrated digital payment grievances with national consumer helpline platform of Department of Consumer Affairs in addition to the existing grievance redressal mechanism of digital payments of the respective banks and National Payment Corporation of India (“NPCI”).</li> </ul>
20.	Sumedhanand Saraswati, BJP	<ul style="list-style-type: none"> <li>● Whether the number of digital payments in the country has increased significantly and if so, the details thereof;</li> <li>● The number of digital payments made during each of the last three years, State/UT-wise;</li> </ul> <p>Whether—</p> <ul style="list-style-type: none"> <li>● the Union Government has conducted any comparative study with regard to digital payments in other countries, if so, the details and the outcome thereof; and</li> <li>● appropriate steps have been taken by the Government for security and safety of various platforms for digital transactions</li> </ul>	<p><u>Response</u> by MeitY:</p> <ul style="list-style-type: none"> <li>● Digital payment transactions have observed a significant growth over the last three years.</li> <li>● The transaction details for State/UTs are not maintained, however total number of digital transactions undertaken in the country for financial years 2016-17, 2017-18, 2018-19, 2019-20 (till 27<sup>th</sup> Feb 2020) are 1004 crores, 2071 crores, 3134 crores, 3649 respectively.</li> <li>● The Reserve Bank of India (“RBI”) released a report on “Benchmarking India’s Payment Systems”, which provides a comparative position of the payment system ecosystem in India and usage trends in other major countries.</li> <li>● The study found that India has a strong regulatory system and robust large value and retail payment systems which have contributed to the rapid growth in the volume of transactions in these payment systems.</li> </ul>

		in the country; and if so, the details thereof and if not, the reasons therefor.	<ul style="list-style-type: none"> <li>• There has been substantial growth in e-payments by Government and also in digital infrastructure in terms of mobile networks.</li> <li>• The report, however, notes that India is required to take further efforts to bring down the volume of paper clearing and increase acceptance infrastructure to enhance digital payments.</li> <li>• Please see response to question No. 19.</li> </ul>
--	--	--	--

### B. Questions raised in Rajya Sabha

S.No.	Name of the MP	Question raised	Response by the Government
21.	Dr. Ameer Yajnik, INC	Whether the government has taken any action to curb the increasing number of Android and iPhone applications for making digital payments and creating spam on these platforms.	<p><a href="#">Response</a> by MeitY :</p> <ul style="list-style-type: none"> <li>• NPCI has taken technical and awareness measures for BHIM/UPI including multiple checks on registration process, communication to user while registering any transaction on UPI app, reduced limits for new users and reduced transaction limit for certain payment modes.</li> <li>• RBI launched a scheme ‘Ombudsman Scheme for Digital Transactions, 2019’ on January 31, 2019 to provide for a mechanism of Ombudsman for redressal of complaints against deficiency in services related to digital transactions.</li> <li>• Please see response to question no.19.</li> </ul>
22.	Prabhakar Reddy Vemireddy, YSR Congress	<ul style="list-style-type: none"> <li>• Whether MeitY is revisiting the UPI-based BHIM App;</li> <li>• The details of each of the objectives set when the scheme was launched;</li> <li>• Whether all the objectives have been achieved and if so, the details thereof, objective-wise;</li> <li>• The number of people using BHIM App now, State-wise and month-wise, since its inception; and</li> </ul>	<p><a href="#">Response</a> by MeitY:</p> <ul style="list-style-type: none"> <li>• To encourage digital payments, the BHIM app was launched. It is a UPI based payment interface developed by NPCI which allows real time fund transfer using a single identity like your mobile number or name.</li> <li>• In order to make the app more effective, new features such as offers, donation, multiple accounts, local language support and limit enhancement etc have been incorporated along with enhancement in existing features under BHIM2.0.</li> </ul>

		<ul style="list-style-type: none"> <li>• Whether it is also a fact that the scheme is facing funding crunch since Ministry is managing with only INR 100 crores whereas it has approved INR 500 crores when scheme was launched.</li> </ul>	<ul style="list-style-type: none"> <li>• NPCI conducted a pilot launch of UPI system on 11th April 2016. Banks started to upload their UPI enabled Apps from 25th August, 2016 and BHIM app was launched on 30th December, 2016.</li> <li>• The main purpose of BHIM App was to provide uniform experience of UPI and also to support those banks who have not developed any UPI app for their customers. The App is a bank agnostic app for online person to person funds transfer and is available on Android and iOS platforms.</li> <li>• State wise data is not available with MeitY.</li> <li>• Promotion of BHIM app is a part of ‘promotion of digital payments’ scheme by MeitY.</li> <li>• There is no funding crunch for promotion of Digital payments.</li> </ul>
--	--	---	---

### III. QUESTIONS ON AADHAAR

#### A. Questions raised in Lok Sabha

S.No.	Name of the MP	Question raised	Response by the Government
23.	Arvind Dharmapuri, BJP	Whether the Government has— <ul style="list-style-type: none"> <li>• taken note of the rampant Aadhaar Fraud in the Kalyana Lakshmi Shaadi Mubarak Welfare Scheme introduced by the Telangana Government;</li> <li>• initiated any investigation in this regard and if so, the details and the outcome thereof; and</li> <li>• The steps taken/being taken by the Government to stop such misuse of Aadhaar data.</li> </ul>	<a href="#">Response</a> by MeitY: <ul style="list-style-type: none"> <li>• The Government of Telangana has not reported any Aadhaar fraud in the Kalyana Lakshmi / Shaadi Mubarak Scheme.</li> <li>• Steps taken by the government to stop misuse of Aadhaar data:                             <ul style="list-style-type: none"> <li>○ Unique Identification Authority of India (“<b>UIDAI</b>”) has a well-designed, multi-layer robust security system in place for ensuing security of Aadhaar data. The same is constantly upgraded to maintain highest level of data security and integrity.</li> <li>○ For further strengthening of security and privacy of data, security audits are conducted on regular basis.</li> <li>○ The security assurance of Aadhaar ecosystem has been strengthened with enactment of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (“<b>Aadhaar Act</b>”). Subsequently the Aadhaar and Other Laws (Amendment) Act, 2019 was enacted with stringent penalties/punishments for offenders in place.</li> <li>○ UIDAI has been declared ISO 27001:2013 certified with respect to information security, which has added another layer of IT security assurance.</li> <li>○ UIDAI has also been declared as protected system by National Critical Information Infrastructure Protection Centre in pursuance of section 70(1) of the IT Act.</li> </ul> </li> </ul>
24.	Rajendra Agrawal, BJP	<ul style="list-style-type: none"> <li>• The number of Aadhaar Seva Kendras (“<b>ASKs</b>”) operationalised by UIDAI across the country, State/UT-wise;</li> </ul>	<a href="#">Response</a> by MeitY: <ul style="list-style-type: none"> <li>• As on 03.03.2020, 35 ASKs are operational across the country. State/UT wise list is attached with Annexure to the question.</li> <li>• Districts in UP where ASKs are planned and operational- Lucknow and Agra (Operational); Meerut, Allahabad, Ghaziabad, Gonda,</li> </ul>

		<ul style="list-style-type: none"> <li>• The districts in Uttar Pradesh (“UP”), where such ASKs have been planned or operationalised;</li> <li>• The number of Aadhaar enrolment/updation requests ASKs can undertake in a day;</li> <li>• Whether the Government has received complaints regarding issues of server slowdown and long pendency of Aadhaar updation requests from such ASKs; and</li> <li>• if so, the details thereof including number of such complaints received by the Government during each of the last three years, State/UT-wise and the steps taken by the Government in this regard.</li> </ul>	<p>Gorakhpur, Kanpur Dehat, Moradabad, Saharanpur and Varanasi (Planned).</p> <ul style="list-style-type: none"> <li>• Three models of ASKs are planned with capacity to undertake requests as under:                         <ul style="list-style-type: none"> <li>○ Model A (with 16 work stations)- 1,000 requests/day</li> <li>○ Model B (with 8 work stations) - 500 requests/day</li> <li>○ Model C (with 4 work stations) - 250 requests/day</li> </ul> </li> <li>• The government has not received any complaints regarding issues of slowdown of servers.</li> </ul>
25.	Y. Devendrappa, BJP	<ul style="list-style-type: none"> <li>• Whether Aadhaar data contains both core biometric information and other demographic information of citizens and if so, the details thereof;</li> <li>• The instances of Aadhaar database breach including core biometric and other demographic information reported during each of the last three years and the current year, State/UT-wise;</li> <li>• The steps taken by the Government in this regard; and</li> <li>• Whether the breach of Aadhaar demographic information is harmful for the citizens and if so, the details thereof and the reasons therefor.</li> </ul>	<p><a href="#">Response</a> by MeitY:</p> <ul style="list-style-type: none"> <li>• During enrolment for Aadhaar, only following minimum information is collected as per regulations 3, 4 and 5 of Aadhaar (Enrolment and update) Regulations 2016:-                         <ul style="list-style-type: none"> <li>○ Biometric Information including facial image, all ten fingerprints and scans of both irises.</li> <li>○ Demographic Information including name, date of birth, gender, residential address, mobile number (optional) and email address (optional).</li> </ul> </li> <li>• There has not been any instance of data breach from Aadhaar database-Central Identities Data Repository (“<b>CIDR</b>”).</li> <li>• Please see response to question no.23.</li> <li>• There are multiple layers of security at physical level in UIDAI Data Centres and is being managed by armed CISF personnel round the clock.</li> </ul>

			<ul style="list-style-type: none"> <li>No information relating to bank account, shares, mutual funds, financial and property details, health records, family, caste, religion, education etc. is stored in Aadhaar database.</li> </ul>
26.	Gopal Jee Thakur, BJP	Whether the— <ul style="list-style-type: none"> <li>Aadhaar card is mandatory for all;</li> <li>government has taken note of the fact that general public is reportedly facing problems due to non-availability of appropriate number of Aadhaar centres in their vicinity and if so, the details thereof and the reasons therefor along with the steps taken by the government in this regard;</li> <li>the government proposes to open Aadhaar centres in every panchayat across the country and if so, the details thereof; and</li> <li>The time by which the said centres are likely to be opened.</li> </ul>	<a href="#">Response</a> by MeitY: <ul style="list-style-type: none"> <li>There are over 41,000 Aadhaar Enrolment and Update Centres across the country functioning in designated Bank branches, Post Offices, etc.</li> <li>UIDAI has opened 35 ASK with facility of online appointment and queue management system which remains open all seven days of the week.</li> <li>UIDAI has provided online facility to update address through its website.</li> <li>As all State Governments are UIDAI's registrars, they are encouraged to open more Aadhaar Kendras in government premises including Panchayat Office.</li> </ul>

### B. Questions raised in Rajya Sabha

S.No.	Name of the MP	Question raised	Response by the Government
27.	K.V.P. Ramachandra Rao, INC	<ul style="list-style-type: none"> <li>Whether the UIDAI has failed to take sufficient precautions to safeguard Aadhaar data of people;</li> <li>if so, the details thereof and if not, how it came to notice of the UIDAI that some private companies are having Aadhaar data of people of Andhra Pradesh and Telangana resulting in registering a case;</li> </ul>	<a href="#">Response</a> by MeitY: <ul style="list-style-type: none"> <li>The data protection system of UIDAI is robust and highly secure.</li> <li>There have been no instances of data theft from UIDAI database CIDR.</li> <li>Based on field inputs, a complaint was lodged by the UIDAI and was registered vide FIR no.278/2019 on 12.04.2019 at Madhapur Gutalla PS, Cyberabad against Management of M/s IT Grids India Pvt Ltd and Others.</li> </ul>

		<ul style="list-style-type: none"> <li>• Whether any in-house enquiry was conducted and whether it identified any officials responsible for the incident, if so, what action was taken against them; and</li> <li>• What precautions the UIDAI has taken to restrict such breach in future.</li> </ul>	<ul style="list-style-type: none"> <li>• No in-house enquiry was conducted by the UIDAI. The case is under investigation by Special Investigation Team comprising of senior police officers of the Government of Telangana.</li> </ul>
28.	K.V.P. Ramachandra Rao, INC	Whether— <ul style="list-style-type: none"> <li>• the government is confident about the safety of biometric data of people secured while collecting Aadhaar data;</li> <li>• several states are sharing Aadhaar data with private companies for identification of beneficiaries under various welfare schemes implemented by them; and</li> <li>• the government has imposed any restrictions on sharing of Aadhaar data with private companies managing data of Government welfare schemes.</li> </ul>	<u>Response</u> by MeitY: <ul style="list-style-type: none"> <li>• Please see response to question no. 23.</li> <li>• There are multiple layers of security at physical level in UIDAI Data Centres and is being managed by armed CISF personnel round the clock.</li> <li>• No instances of states sharing Aadhaar data with private companies has come to the notice of UIDAI.</li> <li>• Provisions under the Aadhaar (Sharing of Information) Regulations, 2016 are invoked to deal with restrictions on sharing, circulating or publishing of Aadhaar number.</li> </ul>



**IV. QUESTIONS ON DATA PROTECTION**
**A. Questions raised in Lok Sabha**

S.No.	Name of the MP	Question raised	Response by the Government
29.	Ram Shankar Katheria, BJP	<ul style="list-style-type: none"> <li>• Whether the government has set up any committee or an agency for protection of personal data; and</li> <li>• The number of complaints received by the government for breach of personal data during each of the last three years, State/UT wise.</li> </ul>	<p><a href="#">Response</a> by MeitY:</p> <ul style="list-style-type: none"> <li>• A committee of experts on data protection under the chairmanship of Justice B N Srikrishna (“<b>Srikrishna Committee</b>”), to study various issues relating to data protection, was set up. The said committee submitted its report and a draft bill.</li> <li>• The said draft bill was placed in public domain for comments. After certain modifications, the PDP Bill was introduced in the Parliament during the winter session 2019.</li> <li>• The PDP Bill has been referred to a Joint Parliamentary Committee (“<b>JPC</b>”) for review.</li> <li>• MeitY has not received any specific complaint pertaining to personal data breach.</li> </ul>
30.	K. Muraleedharan, INC	<p>Whether the government —</p> <ul style="list-style-type: none"> <li>• has made its stand clear with respect to data imperialism and data sovereignty to all countries;</li> <li>• opines that the data protection law must be technology agonistic based on element of free consent, requisite data protection authorities and a fair mechanism for data processing; and</li> <li>• The response received by the Government on its point of view on data imperialism, data sovereignty and data protection law.</li> </ul>	<p><a href="#">Response</a> by MeitY:</p> <ul style="list-style-type: none"> <li>• The essential principles behind the draft law are that it is technology agnostic, promotes holistic application, stresses informed consent, proposes data minimization, lays down controller accountability &amp; structured enforcement and provides for deterrent penalties.</li> <li>• The Justice Srikrishna Committee undertook a wide consultation process and included various points of views before it submitted its report.</li> <li>• Most respondents have welcomed the approach taken by the Committee towards developing a legislation for data protection.</li> <li>• In chapter 2 of its report, the Justice Srikrishna Committee discussed all aspects relating to transferability of data across national borders and the need for legislation to govern jurisdiction over personal data.</li> </ul>
31.	K. Shanmuga	Whether—	<a href="#">Response</a> by MeitY:

	Sundaram, DMK	<ul style="list-style-type: none"> <li>the government has received any report from Justice B.N. Srikrishan Committee on data protection along with draft legislation on data protection and if so, the details thereof;</li> <li>the report categorises data into personal and non-personal data (“NPD”) along with the identification of super sensitive data;</li> <li>the government has accepted the classification of personal data; and</li> <li>the government will include NPD in the proposed legislation on data protection</li> </ul>	<ul style="list-style-type: none"> <li>Please see response to question no.29.</li> <li>Chap 8 of its report, the Justice Srikrishna Committee, contains classification of personal data into sensitive and critical personal data. In the PDP Bill 2019, similar classification of personal data has been made by the government.</li> <li>In the draft PDP Bill 2019 there is an enabling Clause 91 that facilitates use of NPD by the government as an input for policy making process.</li> </ul>
--	---------------	--	--

#### B. Questions raised in Rajya Sabha

S.No.	Name of the MP	Question raised	Response by the Government
32.	A. K. Selvaraj, All India Anna Dravida Munnetra Kazhagam (“AIADMK”)	Whether — <ul style="list-style-type: none"> <li>India has made it clear that any attempt of data imperialism would not be accepted;</li> <li>India has urged all concerned that data sovereignty of all the countries must be respected; and</li> <li>the data protection law must be technology agonistic, based on element of free consent, requisite data protection authorities and a fair mechanism for data processing and if so, the response that government has got on its point of view on data.</li> </ul>	<a href="#">Response</a> by MeitY: <ul style="list-style-type: none"> <li>Please see response to question no. 29 and 30.</li> </ul>

33.	Roopa Ganguly, BJP	<ul style="list-style-type: none"> <li>• The manner in which the National Digital Health Blueprint (“<b>NDHB</b>”) will help the healthcare sector;</li> <li>• Whether there is any merit to the fear of data privacy associated with the NDHB, if so, the details thereof; and</li> <li>• The details of measures being taken by Government to ensure data security.</li> </ul>	<p><u>Response</u> by the Ministry of Health and Family Welfare (“<b>MoHFW</b>”):</p> <ul style="list-style-type: none"> <li>• The NDHB aims to facilitate creation of longitudinal Electronic Health Record (“<b>EHR</b>”) of patient across health facilities breaking silos of data. The implementation of NDHB principles will facilitate robust health data analytics for timely decision making.</li> <li>• NDHB proposes for regulatory requirements to be built into the design of Digital Health Ecosystem a priori, rather than being retrofitted. It also proposes to achieve these complex and mandatory requirements through a combination of building blocks, particularly consent manager, anonymizer and security and privacy operations centre.</li> <li>• NDHB also advocates for “Ensure security and privacy by design” and proposed for a national policy on security of health systems and privacy of personal health records which will be developed under NDHB.</li> <li>• All the building blocks that require handling personal health records will be designed to comply with such policy ab-initio. The National Digital Health Mission (“<b>NDHM</b>”) will facilitate the anonymization of data and consent framework through appropriate software, utilities, hardware etc. ensuring conformance to NDHB principles.</li> </ul>
-----	--------------------	--	--

**V. QUESTIONS ON CYBER SECURITY**
**A. Questions raised in Lok Sabha**

S.No.	Name of the MP	Question raised	Response by the Government
34.	V.K Sreekandan, INC	<ul style="list-style-type: none"> <li>• Whether the government has sent an alert to all states warning them about the vulnerability of the Android operating system to a bug called ‘Strand Hogg’ that allows real time malware applications to pose as genuine applications and access user’s data of all kind;</li> <li>• Steps taken by the government in this regard;</li> <li>• Whether a detailed list of the modus operandi of the hackers and latest trends in cyberattacks has been sent by the government for appropriate action by the states; and</li> <li>• If the government has received any response by the state governments.</li> </ul>	<p><a href="#">Response</a> by MeitY:</p> <ul style="list-style-type: none"> <li>• CERT-In published a vulnerability note on the issue Strand Hogg on 9th December 2019 and alerted the users regarding precautionary measures to be taken.</li> <li>• The government adopted the following measures to check malicious apps and enable users to protect their mobile phones:                             <ul style="list-style-type: none"> <li>○ Alerts and advisories about the threats, vulnerabilities and malware affecting mobile phones along with countermeasures are issued by CERT-In.</li> <li>○ Operationalisation of the Cyber Swachhta Kendra to enable detection and cleaning of malicious code including from mobile / smart phones.</li> <li>○ MeitY regularly conducts programs to generate information security awareness.</li> </ul> </li> <li>• Formulation of guidelines on crisis management plan for countering cyberattacks and cyber terrorism for implementation by all ministries/ departments of central government, state governments and their organizations and critical sectors.</li> </ul>
35.	S. Muniswamy, BJP	Whether the Government plans to conduct WhatsApp security system audit and if so, the details thereof.	<p><a href="#">Response</a> by MeitY:</p> <ul style="list-style-type: none"> <li>• Government has sought submission of information from WhatsApp including discussing the need to conduct an audit of its security systems and processes.</li> </ul>
36.	S. Muniswamy, BJP	<ul style="list-style-type: none"> <li>• Whether the Government plans to set up any authority for cyber security in the country;</li> </ul>	<p><a href="#">Response</a> by MeitY:</p> <p>The government has established the National Critical Information Infrastructure Protection Centre (“<b>NCIIPC</b>”) for protection of critical information infrastructure in the country and the CERT-In for incident response, under the provisions of IT Act.</p>

		<ul style="list-style-type: none"> <li>• If so, the details thereof and the steps taken / being taken by the government in this regard; and</li> <li>• The composition of the said authority along with the criteria laid down by the government for the selection in the said authority.</li> </ul>	
37.	A.K.P. Chinraj, DMK	<ul style="list-style-type: none"> <li>• The MP sought details of the authority responsible for issuing the National Information Security Policy and Guidelines;</li> <li>• Whether any decision has been taken to revise the guidelines in the cyber and information security; if so, the details thereof; and</li> <li>• The time by which it is likely to come into effect.</li> </ul>	<p><a href="#">Response</a> by MHA:</p> <ul style="list-style-type: none"> <li>• Cyber and Information Security measures are taken as per provisions of the IT Act and rules made there under.</li> <li>• MHA issued the National Information Security Policy and Guidelines (“NISP”) in 2019. The Guidelines are revised from time to time as per functional requirements and risk assessment.</li> <li>• The NISP includes measures for strengthening network and infrastructure security; physical security; application security; data security; personnel security; threat and vulnerability management; security and incident management; identity, access and privilege management, etc.</li> </ul>
38.	Locket Chatterjee, BJP	<p>Whether the Government has taken any steps to promote—</p> <ul style="list-style-type: none"> <li>• start-ups in cyber security and if so, details thereof; and</li> <li>• this sector and if so, details thereof.</li> </ul>	<p><a href="#">Response</a> by MeitY:</p> <ul style="list-style-type: none"> <li>• Government has taken the following steps to promote start-ups in cyber security in the country:                         <ul style="list-style-type: none"> <li>○ In Dec 2019, MeitY notified Public Procurement (Preference to Make in India) Order 2019 for cyber security products to encourage ‘Make in India’ and to promote manufacturing of cyber security products in the country.</li> <li>○ In Jan 2020, MeitY launched the Cyber Security Grand Challenge for startups to promote innovation and entrepreneurship culture and build key capabilities in the country in the domain of cyber security.</li> <li>○ MeitY along with Data Security Council of India is implementing a project namely “Cyber Security Technology Development and Centre of Excellence” with the objective of—</li> </ul> </li> </ul>

			<ul style="list-style-type: none"> <li>○ translating existing R&amp;D outcomes to products for wider proliferation;</li> <li>○ development of ecosystem of cyber security technology development and entrepreneurship including start-ups.</li> </ul>
--	--	--	---

**B. Questions raised in Rajya Sabha**

<b>S.No.</b>	<b>Name of the MP</b>	<b>Question raised</b>	<b>Response by the Government</b>
39.	Ameesha Yadav, INC	Whether— <ul style="list-style-type: none"> <li>• cybercrime has increased in the country and if so, steps taken by the government to check it;</li> <li>• the government is considering to impart training to the officers of law enforcing agencies to check cybercrime and for digital forensics etc. in view of the increasing incidents of cybercrime in the country.</li> </ul>	<u>Response</u> by MeitY: <ul style="list-style-type: none"> <li>• As per the data maintained by National Crime Records Bureau (“NCRB”) and the MHA, a total of 12317, 21796 and 27248 cybercrime cases were registered during the years 2016, 2017 and 2018 respectively.</li> <li>• Government has taken legal, technical and administrative measures to prevent cybercrimes including:                             <ul style="list-style-type: none"> <li>○ National Cyber Crime Reporting Portal (“NCRP”) has been launched to enable citizens to report complaints pertaining to all types of cybercrimes.</li> <li>○ The MHA has set up Indian Cyber Crime Coordination Centre in New Delhi to provide a framework and ecosystem for LEAs to deal with cybercrimes in coordinated and comprehensive manner.</li> <li>○ The MHA has developed training curriculum, for LEAs, public prosecutors and judicial officers, covering basic to advanced concepts in cybercrime investigations and forensics.</li> <li>○ The training will help participants to develop knowledge &amp; skills required to understand the nature of cybercrimes &amp; computer forensics and to handle the investigation and prosecution properly. So far, more than 9500 police personnel, judicial officers and public prosecutors have been trained by States/UTs.</li> </ul> </li> </ul>

40.	Veerendra Kumar, Independent MP	<ul style="list-style-type: none"> <li>• Whether the instances of cybercrimes and hacking of Indian websites from foreign countries have increased in recent years and if so, the details and number of such instances reported over the past five years; and</li> <li>• the safeguards in place to prevent cybercrimes and hacking of Indian websites by foreign countries.</li> </ul>	<p><u>Response</u> by MeitY:</p> <ul style="list-style-type: none"> <li>• As per the information reported to and tracked by CERT-In, a total number of 27205, 33147, 30067, 17560 and 21768 Indian websites were hacked during the year 2015, 2016, 2017, 2018 and 2019 respectively.</li> <li>• According to the logs analysed and made available to CERT-In, the Internet Protocol (IP) addresses of the computers from where the attacks appear to be originated belong to various countries including Algeria, China, France, Netherlands, Pakistan, Russia, Serbia, Taiwan, Tunisia etc.</li> <li>• The government has adopted the following measures to prevent cybercrimes:                     <ul style="list-style-type: none"> <li>○ CERT-In devises response measures in coordination with its counterpart agencies in foreign countries involving incidents from outside the country.</li> <li>○ All the government websites and applications are audited with respect to cyber security prior to and after their hosting on a regular basis.</li> <li>○ 90 security auditing organisation to support and audit implementation of Information Security Best Practices.</li> <li>○ Government has formulated Crisis Management Plan for countering cyberattacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.</li> <li>○ Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 44 such drills have so far been conducted by CERT-In where 265 organisations from different States and sectors participated.</li> <li>○ CERT-In conducts regular training programmes for network / system administrators and CISOs of Government and critical sector organisations regarding securing the IT infrastructure and</li> </ul> </li> </ul>
-----	------------------------------------	---	--

			mitigating cyberattacks. 23 trainings covering 692 participants conducted in the year 2019. <ul style="list-style-type: none"> <li>○ Government has set up National Cyber Coordination Centre (“NCCC”) to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities. Phase-I of NCCC has been made operational.</li> </ul>
41.	Sanjay Seth, BJP	Whether the government has — <ul style="list-style-type: none"> <li>• sanctioned a scheme for establishment of Indian Cyber Crime Coordination Centre to handle issues related to cybercrime in the country and the details of the State Governments that have agreed to set up Regional Cyber Crime Coordination Centres; and</li> <li>• setup the NCRP, if so, the number of cases reported and action taken in this regard.</li> </ul>	<u>Response</u> by MHA: <ul style="list-style-type: none"> <li>• ‘Indian Cyber Crime Coordination Centre (I4C)’ scheme has been rolled out to combat cybercrime in the country, in a coordinated and effective manner.</li> <li>• The scheme has seven components including National Cybercrime Threat Analytics Unit, National Cybercrime Reporting Portal, Platform for Joint Cybercrime Investigation Team, National Cybercrime Forensic Laboratory Ecosystem etc.</li> <li>• 21 States/UTs have agreed to setup the regional cybercrime coordination centres.</li> <li>• NCRP was operationalised on 30th August, 2019 and the complaints reported are dealt by LEA of the concerned State/UT as per provisions of the law.</li> <li>• 33,152 cybercrime incidents have been reported till 30.01.2020 on the portal, wherein 790 FIRs have been registered by the concerned LEAs.</li> </ul>
42.	Sukhram Singh Yadav, Samajwadi Party (“SP”) Vishambhar Prasad Nishad, SP Chhayaverma, INC	<ul style="list-style-type: none"> <li>• The details of increase in cybercrimes during the last three years</li> <li>• Whether in view of rising numbers of cybercrimes, the government is heading towards developing a technology which can prevent various crimes in cyber world and a quick monitoring is possible; and</li> <li>• Mechanism available to compensate interests of bank account holders in case of</li> </ul>	<u>Response</u> by MeitY: <ul style="list-style-type: none"> <li>• A total of 12317, 21796 and 27248 cybercrime cases were registered during the years 2016, 2017 and 2018, respectively.</li> <li>• The MHA and MeitY have launched programs to spread awareness on cybercrimes.</li> <li>• Please see response to question no. 39.</li> <li>• To compensate bank account holders in case of economic fraud through cybercrime, the RBI issued various instructions in respect of</li> </ul>



		occurrence of economic fraud through cybercrime.	security and risk mitigation measures related to electronic/digital transactions.
43.	Vivek K. Tankha, INC	<ul style="list-style-type: none"> <li>• Whether the Pegasus Software that permits unauthorized access to mobile phone via security vulnerability in Whatsapp has been purchased by any Government agency / department; and</li> <li>• the reasons for authorization of such purchase which directly infringes upon the Fundamental Right to Privacy under Article 21 of the Constitution.</li> </ul>	<a href="#">Response</a> by MeitY: MeitY has no such information.
44.	Digvijaya Singh, INC	Whether— <ul style="list-style-type: none"> <li>• Facebook had sent a list of WhatsApp users in India whose phones, mails and social media accounts had been hacked by Pegasus spyware owned by NSO, an Israeli company; and</li> <li>• The Minister would inform all those WhatsApp users so that they can also file cases against either Facebook or NSO.</li> </ul>	<a href="#">Response</a> by MeitY: <ul style="list-style-type: none"> <li>• MeitY on 31.10.2019 sought a report from WhatsApp regarding breach of privacy of citizens of India on its messaging platform.</li> <li>• WhatsApp in its reply communicated the aspects relating to exploitation of a vulnerability in their platform by a spyware called Pegasus, developed by Israeli company NSO Group.</li> <li>• WhatsApp also informed that it is believed that around 1400 users’ devices were attempted to be attacked globally including 121 users in India. It further stated that personal data of approx. 20 users in India might have been breached.</li> <li>• No details of the affected Indian users were shared by WhatsApp.</li> </ul>
45.	Kanwar Deep Singh, AITC	Whether the Government has— <ul style="list-style-type: none"> <li>• undertaken wide-scale campaigns to make public aware about cyber threats like data theft, phishing and ransomware attacks and if so, the details thereof;</li> <li>• has maintained State-wise data on effectiveness of these campaigns in reducing cyber crimes and if so, the details thereof; and proposes to introduce a 24x7</li> </ul>	<a href="#">Response</a> by MeitY: <ul style="list-style-type: none"> <li>• Please see response to question no.1</li> <li>• CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on regular basis.</li> <li>• To spread awareness on cyber crime, MHA has taken several steps including publishing of ‘Information Security Best practices’ for the benefit of Govt. Officials, organizing of Cyber Safety and Security</li> </ul>

		<p>nationwide cyber security helpline number to specifically deal with cyber crimes and if so, the details thereof.</p>	<p>Awareness weeks in association with police department in different States/UTs etc.</p> <ul style="list-style-type: none"> <li>• Please see response to question no. 39 and 40.</li> <li>• MeitY does not maintain state-wise data.</li> <li>• CERT-In operates 24x7 Incident Response Help Desk wherein cyber security incidents can be reported via toll-free telephone number, email or fax</li> </ul>
--	--	---	---

**VI. QUESTIONS ON E-COMMERCE**
**A. Questions raised in Lok Sabha**

S.No.	Name of the MP	Question raised	Response by the Government
46.	Sanjay Sadashivrao Mandlik, Shiv Sena ("SS") Sudheer Gupta, BJP Gajanan Chandrakant Kirtikar, SS Bidyut Baran Mahato, BJP	<ul style="list-style-type: none"> <li>• Whether the government is working on the e-commerce and new industrial policies for setting up a legal and technological framework for restrictions on cross-border data flow and laid certain conditions on processing the sensitive data locally and storing it abroad and if so, details of such policies;</li> <li>• the time by which the said policies are likely to be implemented; Whether—</li> <li>• the Government has held any meeting with various stakeholders in this regard and if so, the details thereof; and</li> <li>• several foreign e-commerce firms have raised concern over a few points in the draft policy pertaining to data and if so, the details thereof and the response of the Government in this regard.</li> </ul>	<p><a href="#">Response</a> by the Ministry of commerce and industry ("MCI"):</p> <ul style="list-style-type: none"> <li>• The National e-commerce policy and the new industrial policy is under consideration of the government.</li> <li>• The draft National e-commerce policy is aimed at empowering domestic entrepreneurs and to encourage Make in India while safeguarding interests of the consumers and facilitating job creation.</li> <li>• The proposed new Industrial policy seeks to boost competitiveness and growth of the manufacturing sector in India.</li> <li>• MeitY has introduced the PDP Bill 2019, which seeks to specify the flow and usage of personal data, defines sensitive data and aims to create a framework for organisational and technical measures in processing of data, laying down norms for cross-border transfer and accountability of entities processing personal data.</li> <li>• Since e-commerce is a new issue, it has necessitated detailed consultations over the last few months to ensure that the policy is crafted in a manner that interests of all stakeholders are taken into account. Therefore, no timeline has been fixed for release of the same.</li> <li>• On the 23rd February, 2019, the first draft of the National e-Commerce policy was placed in public domain and comments from over 120 stakeholders (companies both Indian and foreign, Industry associations, think tanks, foreign governments) were received.</li> <li>• A series of meetings have been held at the level of Secretary, DPIIT with different stakeholders, including major e-commerce companies, start-ups, industry associations, data centre providers, logistics companies, etc. to discuss the issues facing the sector and the provisions contained in the draft Policy.</li> </ul>

			<ul style="list-style-type: none"> <li>• With regard to the new Industrial Policy, a working group has been constituted with representation from Central Ministries/Departments, State Governments, and industry associations.</li> <li>• The Working Group is chaired by Secretary, DPIIT. The first meeting of the Working Group was held on 24th October, 2019 and Inter-ministerial consultation is currently going on for framing the new Industrial Policy.</li> </ul>
47.	Thalikkottai Rajuthevar Baalu, DMK	<ul style="list-style-type: none"> <li>• Whether the government has framed a roadmap to exploit the benefits of the digital economy while safeguarding the interests of all stakeholders.</li> <li>• Details of the initiatives taken by the government on the country's e-commerce policy to tackle cross border data flows.</li> </ul>	<p><a href="#">Response</a> by MCI:</p> <ul style="list-style-type: none"> <li>• The Digital India programme was launched in July 2015 to transform India into a knowledge-based economy and digitally empowered society.</li> <li>• A Report by MeitY titled, "India's Trillion Dollar Digital Opportunity" outlines the measures that will help India to optimally harness digital technologies in the core economic and social sectors.</li> <li>• The National Policy on Electronics ("NPE") and National Policy on Software Products ("NPSP") in 2019 for the growing digital economy have been introduced by the government for growing digital economy.</li> <li>• Please see response to question no.46.</li> <li>• The PDP Bill, currently under review with the JPC, seeks to establish a strong and robust data protection framework for India.</li> <li>• MeitY has constituted a committee of experts to deliberate on the data governance framework relating to NPD.</li> </ul>

#### B. Questions raised in Rajya Sabha

S.No.	Name of the MP	Question raised	Response by the Government
48.	Abhishek Manu Singhvi, INC	Whether the government — <ul style="list-style-type: none"> <li>• can access the personal data of individuals generated from e-commerce;</li> </ul>	<p><a href="#">Response</a> by MCI:</p> <ul style="list-style-type: none"> <li>• After examining various issues related protection of personal data, the Srikrishna Committee released a draft PDP Bill. Based on stakeholders' comments, the PDP Bill was introduced in parliament</li> </ul>

		<p>has received stakeholder responses on National e-commerce Policy, 2019; and</p> <ul style="list-style-type: none"> <li>• has created a policy framework for encouraging the efficiency of domestic e-commerce companies</li> </ul>	<p>during the winter session 2019 and the bill has currently been referred to a JPC for review.</p> <ul style="list-style-type: none"> <li>• Formulation of the national e-commerce policy is under consideration of the Government. The draft policy seeks to create a facilitative regulatory environment for growth of e-commerce sector, is aimed at empowering domestic entrepreneurs and to encourage Make in India while safeguarding interests of the consumers and facilitating job creation.</li> </ul>
--	--	---	---

**VII. QUESTIONS ON EMERGING TECHNOLOGIES**
**A. Questions raised in Lok Sabha**

S.No.	Name of the MP	Question raised	Response by the Government
49.	Supriya Sadanand Sule, Nationalist Congress Party (“NCP”) DNV Senthilkumar. S, DMK Manickam Tagore B, INC Subhash Ramrao Bhamre, BJP Kuldeep Rai Sharma, INC Amol Ramsing Kolhe, NCP Shriniwas Dadasaheb Patil, NCP	<ul style="list-style-type: none"> <li>• Whether the government has organised an Artificial Intelligence (“AI”) summit focused on social empowerment in New Delhi recently, and if so, the details of the issues discussed in the summit; and</li> <li>• the steps taken by the government to promote AI and to make the country a destination for AI based research and development in the world.</li> </ul>	<p><u>Response</u> by MeitY:</p> <ul style="list-style-type: none"> <li>• Government’s plan to hold a summit on AI with focus on social empowerment was delayed due to sudden outbreak of the novel coronavirus disease (“COVID-19”).</li> <li>• Through this summit, the government intended to outline India’s vision for utilizing the power of AI to responsibly transform the social landscape for a better tomorrow.</li> <li>• To promote AI, the government launched a National Mission on Interdisciplinary Cyber Physical Systems (“NM-ICPS”) at a total cost of INR 3,660 Crores for a period of 5 years.</li> <li>• NM-ICPS plans to establish technology innovation hubs in AI, Internet of Things (“IoT”), 3D printing, quantum computing etc.</li> <li>• To promote tech entrepreneurship, the government launched the Technology Incubation and Development of Entrepreneurs (“TIDE 2.0”) scheme. It will provide financial and technical support to incubators engaged in supporting ICT start-ups using emerging technologies such as AI, IoT, block-chain, robotics etc. in areas of social relevance.</li> <li>• To foster innovation and to promote start-ups in the domains of emerging technologies, MeitY has established Centres of Excellence (“CoE”). These centres connect various entities such as start-ups, enterprises, venture capitalists, government and academia to work on various problem areas and develop emerging technologies based solutions.</li> <li>• MeitY through National Informatics Centre (“NIC”) &amp; National Informatics Centre Services Incorporated (“NICSI”) created Centre of</li> </ul>

			Excellence for Data Analytics (“ <b>CEDA</b> ”) to support government departments to unlock the hidden potential of the data that they are generating as a part of the governance processes, and use it to improve the overall governance.
50.	Raja Amareshwara Naik, BJP Sangeeta Kumari Singh Deo, BJP Bhola Singh, BJP Vinod Kumar Sonkar, BJP Sukanta Majumda, BJP Jayanta Kumar Roy, BJP	Whether the government— <ul style="list-style-type: none"> <li>proposes to formulate any policy to enable private sector to build Data Centre Parks throughout the country and if so, the details thereof;</li> <li>has any plan to develop new technologies like AI, IoT, 3D printing, quantum computing, etc. and if so, the details thereof;</li> </ul>	<a href="#">Response</a> by MeitY: <ul style="list-style-type: none"> <li>As per budget announcements for 2020-2021, the government proposes to bring out a policy to build Data Centre Parks throughout the country. This will enable firms to skilfully incorporate data in every step of their value chains.</li> <li>Please see response to question no. 49.</li> </ul>
51.	Jagdambika Pal, BJP	Whether the government proposes to formulate a policy to regulate AI in the country.	<a href="#">Response</a> by MeitY: <ul style="list-style-type: none"> <li>NITI Aayog released the National Strategy for Artificial Intelligence (“<b>NSAI</b>”) in June 2018 outlining India’s proposed efforts in research, development, adoption and skilling in AI.</li> <li>The NSAI discusses setting up of a Task Force led jointly by MeitY and NITI Aayog for the development of a template of the required legal and regulatory framework in the domain of AI.</li> <li>The NSAI details the following barriers:                         <ul style="list-style-type: none"> <li>Lack of broad based expertise in research and application of AI,</li> <li>Absence of enabling data ecosystems – access to intelligent data,</li> <li>High resource cost and low awareness for adoption of AI,</li> <li>Privacy and security, including a lack of formal regulations around anonymization of data, and</li> <li>Absence of collaborative approach to adoption and application of AI.</li> </ul> </li> </ul>

			<ul style="list-style-type: none"> <li>• The NSAI acknowledges that data is one of the primary drivers of AI solutions and thus ensuring privacy and security of such data is of prime importance.</li> <li>• Some of the challenges identified in the NSAI include data usage without consent, risk of identification of individuals through data, data selection bias and the resulting discrimination of AI models, and asymmetry in data aggregation.</li> <li>• The NSAI suggests establishing data protection frameworks and sectoral regulatory frameworks, and promotion of adoption of international standards.</li> </ul>
52.	P.P. Chaudhary, BJP	The MP sought details regarding— <ul style="list-style-type: none"> <li>• implementation of NSAI by NITI Aayog;</li> <li>• status of Centre for Excellence for AI; and</li> <li>• the number of countries NITI Aayog has partnered with for knowledge sharing of AI.</li> </ul>	<a href="#">Response</a> by MeitY: <ul style="list-style-type: none"> <li>• Please see response to question no. 51.</li> <li>• The major recommendations of the strategy include setting up Centres of Research Excellence (“<b>CORE</b>”)- focused on fundamental research; and International Centres on Transformational AI (“<b>ICTAI</b>”)- focused on applied research.</li> <li>• The AI vertical of the NM-ICPS programme of DST will be implemented as per the recommendations of the NSAI.</li> <li>• The details of the implementation mechanism for the NSAI are being finalised.</li> <li>• NITI Aayog has collaborated with the Department for Business, Energy and Industrial Strategy (“<b>BEIS</b>”) of the Government of UK, Ministry of Economy, Trade and Industry (“<b>METI</b>”), Japan, Nanyang Technological University, Singapore and Treasury, Government of Australia.</li> </ul>
53.	Amar Singh, INC	Whether the government has— <ul style="list-style-type: none"> <li>• devised any mechanism to find the right balance between regulation and promotion of emerging technologies;</li> <li>• formulated any action plan for using facial recognition technology in the control of</li> </ul>	<a href="#">Response</a> by MeitY: <ul style="list-style-type: none"> <li>• The adoption of emerging technologies for security forces is a continuous and ongoing process.</li> <li>• The union government adopts and promotes emerging technologies for upgradation of police forces from time to time.</li> </ul>



		crime, better border controls and countering terrorism in the country; and <ul style="list-style-type: none"> <li>has taken any steps in view of the fact that facial recognition is not entirely accurate and could lead to punitive action against innocent people.</li> </ul>	<ul style="list-style-type: none"> <li>The Central Armed Police Forces keep on finalizing Qualitative Requirements (“QRs”) and Trial Directives (“TDs”) as and when the need arises in case of any emerging technology.</li> <li>The state governments also adopt these QRs and TDs for acquisition of the products in such technologies including facial recognition technology.</li> </ul>
--	--	--	--

**B. Questions raised in Rajya Sabha**

S.No.	Name of the MP	Question raised	Response by the Government
54.	B. Lingaiah Yadav, Telangana Rashtra Samithi	<ul style="list-style-type: none"> <li>Whether state government of Telangana is ushering in 2020 as the state's "Year of AI" as the state has been at the forefront of applying emerging technologies such as AI, blockchain;</li> <li>The role of MeitY and NITI Aayog in developing the state in AI; and</li> <li>The steps taken by the government to formulate AI-specific incentives for its overall development in the state.</li> </ul>	<p><a href="#">Response</a> by MeitY:</p> <ul style="list-style-type: none"> <li>The Telangana government has declared 2020 as the year of AI.</li> <li>MeitY, the Telangana government, Software Technology Parks of India (“STPI”) and others are going to establish Centre of Excellence on Gaming, VFX (Visual Effects), computer vision &amp; AI at Hyderabad.</li> <li>Telangana government has signed a Letter of Intent with NITI Aayog on 3 July 2018 to identify AI based projects that can be implemented in the state.</li> <li>No AI-specific incentives have been formulated for Telangana government by the union government.</li> </ul>
55.	Md. Nadimul Haque, AITC	The MP sought details of— <ul style="list-style-type: none"> <li>the total expenditure incurred on development of Internet of Things (“IoT”) devices in the last three years;</li> <li>the IoT device based policies that have been implemented by Government during the last three years and if not, whether the government plans to incorporate such policy measures.</li> </ul>	<p><a href="#">Response</a> by the minister of science and technology:</p> <ul style="list-style-type: none"> <li>The government spent INR 29.29 crores on development of IoT devices in the last three years.</li> <li>The government has not implemented any policy for IoT devices in the last three years.</li> <li>MeitY has already circulated a draft IoT policy which has the vision to develop connected and smart IoT based systems for our country’s economy, society, environment and global needs for public consideration.</li> </ul>

**VIII. MISCELLANEOUS QUESTIONS**
**A. Questions raised in Rajya Sabha**

<b>S.No.</b>	<b>Name of the MP</b>	<b>Question raised</b>	<b>Response by the Government</b>
56.	Md. Nadimul Haque, AITC	Is there a regulatory structure for cloud based services and companies in India and if the Telecom Regulatory Authority of India (“ <b>TRAI</b> ”) is one of the regulators.	<a href="#">Response</a> by MeitY: Presently, no regulatory structure exists for cloud based services and companies in India.
57.	Narain Dass Gupta, Aam Aadmi Party (“ <b>AAP</b> ”)	Whether the ministry is – <ul style="list-style-type: none"> <li>• aware of the perils of deep fake technology often used for political purposes and harassment of women; and</li> <li>• working towards introducing criminal recourse for victims.</li> </ul>	<a href="#">Response</a> by MeitY: <ul style="list-style-type: none"> <li>• The MeitY is aware of perils of deep fake technology</li> <li>• There are adequate legal provisions under the IT Act to prevent the spread of deep fakes.</li> <li>• Please see response to question no.1.</li> </ul>
58.	C.M Ramesh, BJP	<ul style="list-style-type: none"> <li>• Whether the government proposes to review the existing acts and rules relating to pornography and piracy;</li> <li>• When was the last time relevant Acts relating to pornography were reviewed by the government; and</li> <li>• Whether the Ministry proposes to constitute any high level Committee in this regard with a definite time line, the details thereof and if not, the reasons therefor.</li> </ul>	<a href="#">Response</a> by MeitY: <ul style="list-style-type: none"> <li>• There are adequate provisions under the IT Act and the Intermediary Guidelines to deal with the issue of pornography and piracy.</li> <li>• Additionally, several other legislations such as the Protection of Children from Sexual Offences Act, 2012, Indecent Representation of Women Act, 1986, Indian Penal Code have provisions to deal with pornography.</li> <li>• The Copyright Act, 1957 provides for punishment for piracy and copyright violations.</li> <li>• There is no such proposal to constitute any high level committee at this stage.</li> </ul>
59.	A.K.Selvaraj, AIADMK	<ul style="list-style-type: none"> <li>• Whether it is a fact that UIDAI has decided to drop its decision to hire a social media monitoring agency and if so;</li> </ul>	<a href="#">Response</a> by MeitY: <ul style="list-style-type: none"> <li>• The government has dropped the proposal to hire a social media monitoring agency</li> </ul>

		<ul style="list-style-type: none"> <li>• whether the said move was meant to mount surveillance on social media platforms; and</li> </ul>	<ul style="list-style-type: none"> <li>• The tender for hiring such an agency was floated through Central Public Procurement (“<b>CPP</b>”) Portal by UIDAI on 18.07.2018 and was not pursued further and thus automatically cancelled.</li> </ul>
60.	S Muthukaruppan, AIADMK	Whether— <ul style="list-style-type: none"> <li>• social media giants have claimed that journalists, individuals and human rights activists in the country have been targets of surveillance; and</li> <li>• the government has received any representation on this issue asking for a probe under court watch.</li> </ul>	<u>Response</u> by MeitY: <ul style="list-style-type: none"> <li>• Some statements appeared in the media regarding breach of privacy of Indian citizens on WhatsApp.</li> <li>• Such statements attempt to malign the Government of India.</li> <li>• The Government is committed to protect the fundamental rights of citizens, including the right to privacy.</li> <li>• There are adequate safeguards to ensure that no innocent citizen is harassed, or his privacy breached.</li> </ul>
61.	A. K. Selvaraj, AIADMK	Whether— <ul style="list-style-type: none"> <li>• the Automated Facial Recognition System (“<b>AFRS</b>”) is being implemented by the NCRB;</li> <li>• the AFRS will violate privacy; and the database of AFRS would be accessible only to law enforcement agencies.</li> </ul>	<u>Response</u> by MHA: <ul style="list-style-type: none"> <li>• The NCRB has been accorded approval for implementation of AFRS so as to facilitate better identification of criminals, unidentified dead bodies &amp; missing/found children and persons.</li> <li>• AFRS does not violate privacy.</li> <li>• The AFRS uses police records and is accessed only by LEAs.</li> </ul>
62.	M. Shanmugam, DMK	<ul style="list-style-type: none"> <li>• Whether the government proposes to bring out a policy to enable private players to set up data centre parks in the country;</li> <li>• In what way, it would be different from the IT Parks; and</li> <li>• the manner in which it would ensure that such a policy does not violate the right to privacy of individuals.</li> </ul>	<u>Response</u> by MeitY: <ul style="list-style-type: none"> <li>• As per the budget announcement 2020-2021, the government intends to bring out a policy to enable private sector to build data centre parks throughout the country.</li> <li>• IT Parks typically host IT units such as IT companies, Business Processing Office (“<b>BPOs</b>”), Knowledge Processing Outsourcing (“<b>KPOs</b>”), Start-ups and may also host data centres. On the other hand, a Data Centre Park facilitates establishment of Data Centres through private sector participation.</li> <li>• Please see response to question no.29.</li> </ul>