ORF

SWIPING RIGHT ON TECH POLICY

An Assessment of Young India's Aspirations

ANTARA VATS

ANUSHKA SAXENA

RENITA D'SOUZA

Attribution: Antara Vats, Anushka Saxena and Renita D'Souza, *Swiping Right on Tech Policy: An Assessment of Young India's Aspirations*, May 2022, Observer Research Foundation.

Observer Research Foundation
20 Rouse Avenue, Institutional Area
New Delhi 110002
India
contactus@orfonline.org
www.orfonline.org

The Observer Research Foundation (ORF) provides non-partisan, independent analyses and inputs on matters of security, strategy, economy, development, energy and global governance to diverse decision-makers (governments, business communities, academia, and civil society). ORF's mandate is to conduct in-depth research, provide inclusive platforms, and invest in tomorrow's thought leaders today.

Design & Layout: Rahil Miya Shaikh

Cover - rawpixel.com/Hein
Page 8 - Getty Images/Mayur Kakade
Page 11 - Getty Images/Donald Iain Smith
Page 27 - Getty Images/John M Lund Photography
Page 91 - Getty Images/Orbon Alija
Page 94 - Getty Images/MStudioImages
Page 106 - Getty Images/South_agency

Contents

PREFACE

Since the outbreak of the COVID-19 pandemic, technology has become a much more integral part of our lives. We are witnessing an unprecedented growth in the use of technology to stay connected, conduct our daily affairs, and engage in employment. Yet, this development has not been a leveller—not all technology is equal; nor is access to it. There are marked disparities in how populations are able to access technology, across gender, age, region, and level of education. How do we bridge these gaps and build a bigger table as we debate questions on contemporary technology policy?

Technological advancements, the preferences of consumers, and the decisions that developers of technology platforms make, end up influencing and shaping one other. Countries and geographies such as India, the European Union, the United States, and China are all exploring ways by which technology companies can be regulated to protect the security of the state and the safety of its citizens. Ensuring that these strategies are net-positive for society will depend greatly on the choices we will make in the days ahead with respect to the rules, regulations, and legal frameworks that will govern technology.

In India, the youth account for a majority of the users of technology. However, their concerns are largely excluded from current debates even as they intensify their engagement with these platforms and technologies. This first iteration of ORF's technology policy survey—*Swiping Right on Tech*

Policy: An Assessment of Young India's Aspirations, conducted in collaboration with Impetus Research—is an attempt to assess how India's youth understand and relate to the role of technology in their lives. The questions were framed in the context of a global technology order undergoing transformation, with the aim of accounting for issues such as the creation and spread of child sexual abuse material, election interference using emerging technologies, and cyberattacks.

The report explores the youth's support for current proposals on the regulation of data and technology across three parameters—i.e., individual privacy, national sovereignty and security, and economic well-being. The survey explored whether, for India's youth, there exists a "digital trilemma": Do they knowingly or unknowingly give more importance to, or favour two of these values while sacrificing the third? The report finds evidence of such a tendency. An average respondent is more likely to decide in favour of national sovereignty and security, and economic well-being, than against them—as compared to deciding in favour of individual privacy than against it.

On a number of critical issues, the survey results also showed, India's youth have a largely positive attitude towards technology and have, metaphorically, 'swiped right' on the current debates. They are proactive in safeguarding their privacy, and they support the underlying principles of the electronic consent framework. Indeed, more than 80 percent of the respondents agreed with the principles underlying the consent framework, including: user-centricity, trustability and compliance with the Information Technology Act, universal identity, and granular control. They also expressed their willingness to share their locational, medical, and financial data if it is required to bolster economic well-being and public safety. The respondents also expressed support for India becoming a part of international coalitions to deter foreign countries from interfering in domestic elections, or for taking punitive measures against nations that allow hacker groups to operate from within their territories. The report offers specific recommendations to assist India in navigating its policy options.

As nations work to establish accountability mechanisms in the coming years and the use of technology continues to evolve rapidly, ORF is committed to conducting this survey on an annual basis. In future iterations of this survey, we would like to explore public perceptions of the skills required to maximise benefits from the Fourth Industrial Revolution, as well as the possible regulatory approaches for emerging technologies such as artificial intelligence and quantum technology.

Reflecting the themes as well as the goals of the survey, this entire endeavour and the writing of the report were carried out by three young women—Antara Vats, Anushka Saxena, and Dr. Renita D'Souza. My congratulations to the authors in taking up this enormous challenge amidst the pandemic. It is our hope that this survey report has succeeded in capturing important perspectives that will influence, in the coming years, how we address issues around technology and its relation to the state and society.

Dr. Rajeswari Pillai Rajagopalan
Director, ORF's Centre for Security, Strategy and Technology
May 2022

KEY TAKEAWAYS: WHAT INDIA'S YOUTH WANT FROM POLICY DELIBERATIONS ON TECHNOLOGY

1. India's youth have a strong interest in safeguarding their individual privacy. More than eight of every 10 respondents (88 percent) believe that they should be able to determine how their data is shared and used by the government and social media intermediaries.

2. More than seven of every 10 respondents (79 percent) support the right to be forgotten through the mandatory erasure, on a user's request, of their personal information that is collected and processed by private companies.

3. India's youth support data localisation. About 70 percent of the respondents agree with the proposal that foreign enterprises should store and process data within data centres in India.

4. India's youth believe that the government must promote domestic technology and enterprises. Eighty-three percent of the respondents support official policies that would create a protectionist environment for India's technology industry. Meanwhile, 58 percent of the respondents say they rarely or never use Indian alternatives to foreign social media platforms.

5. Respondents support government investments in mobile towers (93 percent), uninterrupted supply of critical mineral resources (88 percent), development of indigenous computer or mobile chips (88 percent), open data regimes for enabling AI innovation (88 percent), and development of indigenous social media platform alternatives or encrypted messaging platforms (88 percent).

6. A majority of the respondents (84 percent) support more severe penalties for foreign companies than for Indian companies for privacy-related offences, even if both have committed similar infractions. More than 86 percent of the respondents agree that the government should impose fines on social media intermediaries that are misused to spread rumours that could potentially challenge the credibility of users or pose a threat to their jobs.

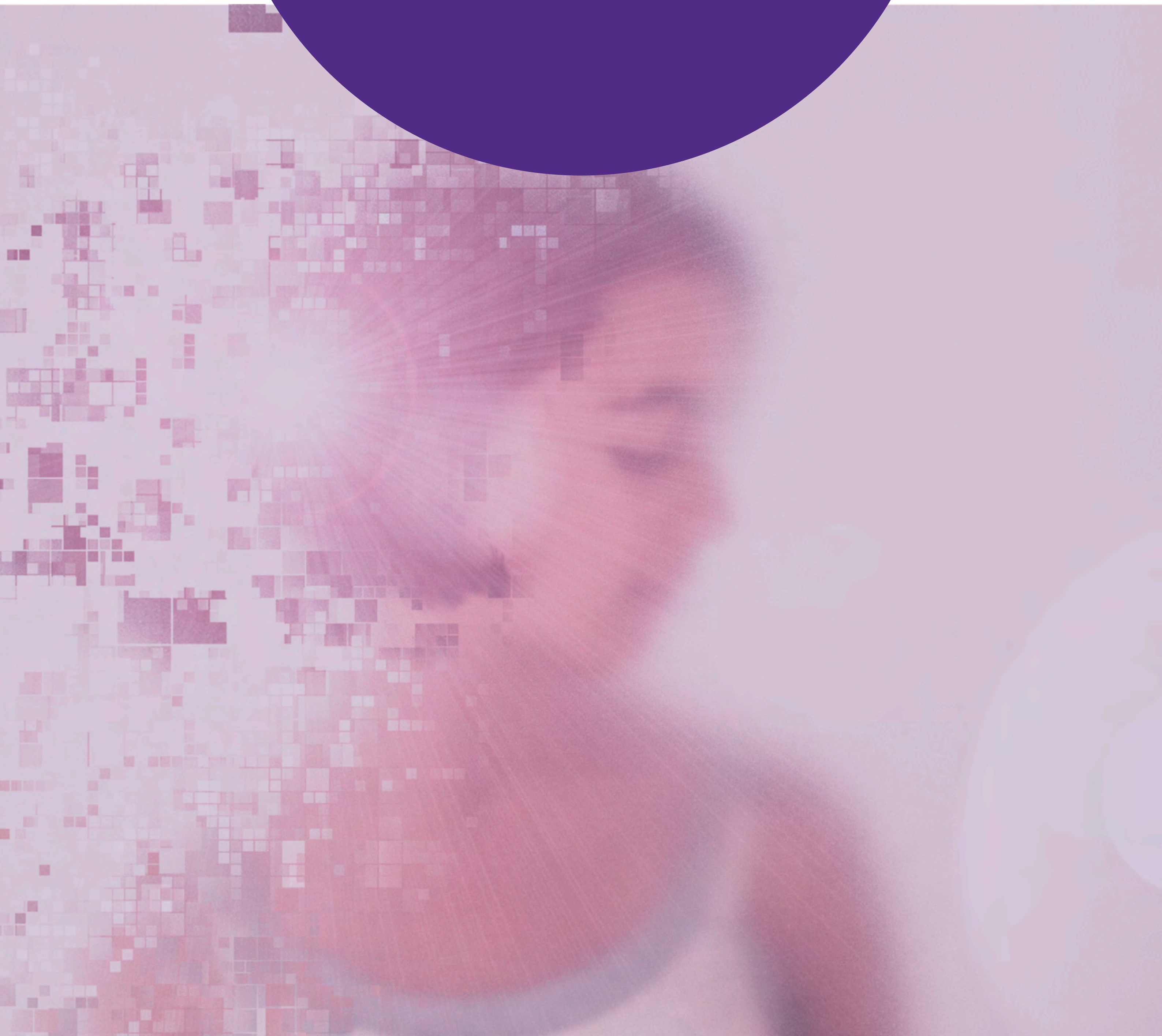
7. India’s youth are largely comfortable sharing their personal data to support government schemes such as providing rations or cash to the poor (82 percent) and for reducing road accidents (79 percent). There is less support for sharing data to assist the Indian government’s anti-terrorism efforts (59 percent). Over 66 percent of respondents are uncomfortable with the proposal of sharing their biometric data in exchange for monetary compensation.

8. Three-fourths of the respondents (77 percent) agree with the idea that the government would prioritise public safety and national security over an individual’s right to privacy.

9. Eight of every 10 respondents (80 percent) support the development of offensive cyber capabilities as part of India’s National Cybersecurity Policy. They also support India becoming a part of international coalitions to deter countries from interfering in another country’s elections (79 percent of respondents). Eighty-eight percent agree that international coalitions should impose punitive measures on countries that allow hacker groups to operate from within their territories.

10. A majority of India’s youth regard the values of individual privacy, national sovereignty and security, and economic well-being, as being of highest importance.

INTRODUCTION



In the past several years, a multitude of technological advancements have become more ubiquitous in people's daily lives. Yet, these technologies are not only driving growth but provoking anxieties as well. Since early 2020, the COVID-19 pandemic has highlighted the role of technological connectivity in making economies function, improving socio-economic capabilities, and closing the gender gap in accessing services. At the same time, concerns are growing about issues such as state-sponsored cyberattacks, digital surveillance by foreign entities, and violations of user privacy. Indeed, the fast digitalising world is expected to become even more complex, and the burden will be borne largely by the younger generations.

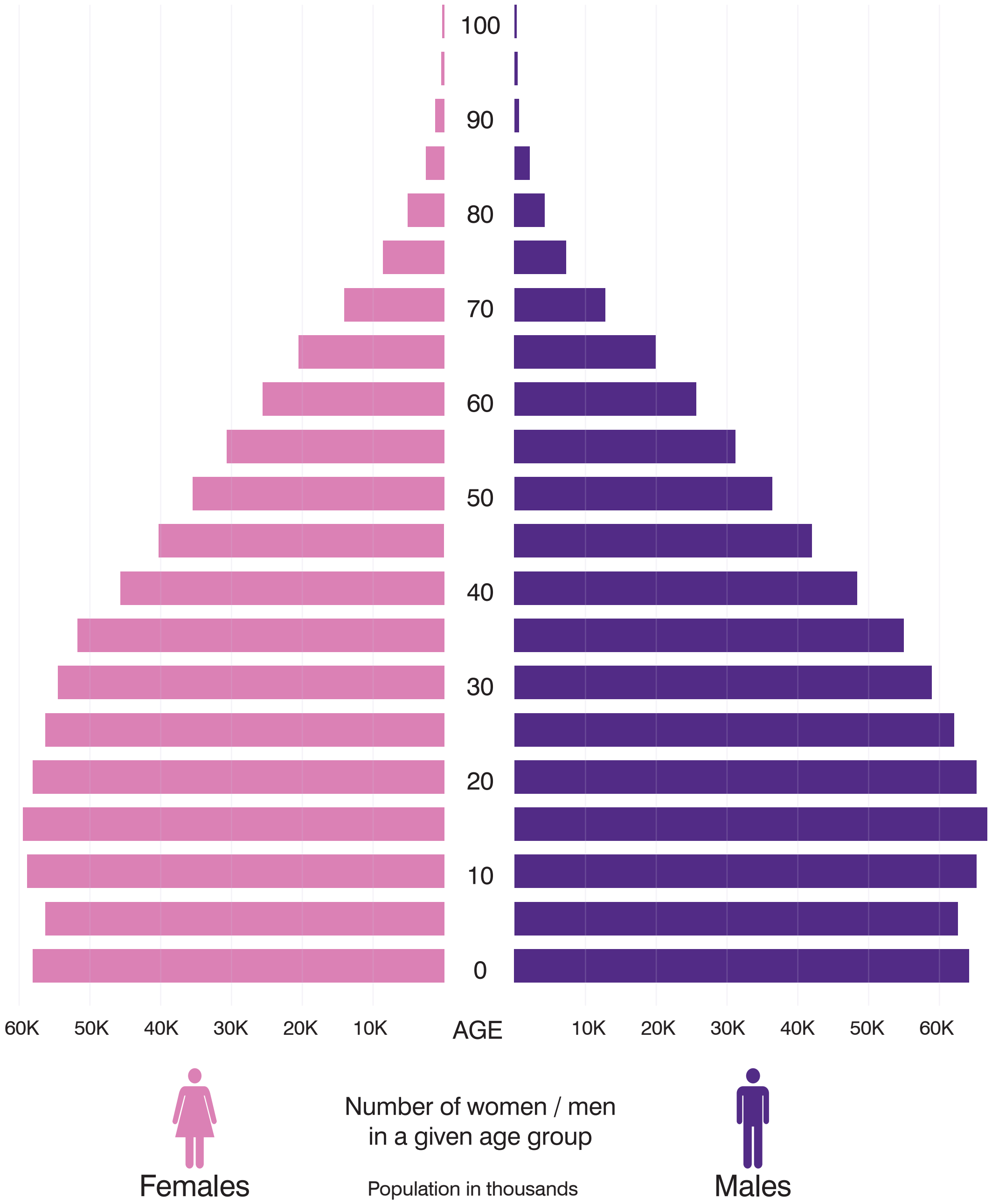
India, with over 624 million[1] internet users in January 2021, is the second largest and fastest[2] growing online market globally, ranked only behind China. India had around 448 million social media users in January 2020 and registered an increase of 78 million between 2020 and 2021. The number of internet users in the country is expected to reach 900 million by 2025. At present, the majority of internet users in India are between 20 and 29 years old, and use the Internet to access Edtech and social media platforms.[3] India is also home to one of the youngest populations in the world, with an average age of 29 years (See Figure 1). Among other factors, the youth's engagement with technological advancements will play a huge role in facilitating India's economic growth in the coming years.[4]

[1] Simon Kemp, *Digital 2021: India.* Data Reportal, 2021, https://datareportal.com/reports/digital 2021-india.

[2] KANTAR and IAMAI, *Internet Adoption in India - ICUBE 2020*, 2021, https://images.assettype.com/afaqs/2021-06/b9a3220f-ae2f-43db-a0b4-36a372b243c4/KANTAR_ICUBE_2020_Report_C1.pdf.

[3] Sandhya Keelery, *Internet Usage in India - statistics & facts, Statista*, https://www.statista.com/topics/2157/internet-usage-in-india/#dossierKeyfigures.

Figure 1. India's Demographic Dividend (2022)



Source: United Nations Population Fund, https://www.unfpa.org/data/demographic-dividend/IN

Data is the foundation on which digital economies are built. In policy discourses, values of individual dignity and liberty,[5] national asset,[6] and economic resource[7] are assigned to data.

[4] Ministry of External Affairs,"One of The Youngest Populations in the World – India's Most Valuable Asset," *Economic Diplomacy Division*, June 13, 2021, https://indbiz.gov.in/one-of-the-youngest-populations-in-the-world-indias-most-valuable-asset/.

These competing characterisations of data based on values have often muddled policy proposals for regulation. In this report, the authors explore how India's youth understand the role of technology in their lives and relate to it. The analysis primarily uses data collected from a survey that investigates their support for proposals on the regulation of data and technology across three parameters: individual privacy, national sovereignty and security, and economic well-being. The authors also use secondary sources to corroborate the survey findings and develop a comprehensive context for the reader.

This report has a threefold aim:

1. To measure the awareness of India's youth on the approaches adopted by consumers, commercial entities, and states to enhance cybersecurity and individual privacy.
2. To identify the concerns of India's youth around the domestic and international approaches adopted for the regulation of technology vis-à-vis individual privacy, economic well-being, and national sovereignty and security.
3. To gauge the opinions of India's youth on future policy options as the country seeks to level concerns around individual privacy, economic well-being, and national sovereignty and security.

[5] V. Shivshankar, "Privacy and Essential Aspects of Human Dignity, says Supreme Court in Historic Ruling," *The Wire*, August 24, 2017, https://thewire.in/law/supreme-court-right-to-privacy-verdict.

[6] Simon Hansford, "Data must be treated as a national asset," *Public Technology*, January 10, 2020, https://www.publictechnology.net/articles/opinion/data-must-be-treated-national-asset.

[7] The Indian Express, "Data is an economic resource. Gopalakrishnan committee report shows how its value can be shared, governed," July 27, 2020, https://indianexpress.com/article/opinion/data-sharing-digital-world-gopalakrishnan-committee-6524049/.

Context and Rationale of the Survey

Perception surveys around technology policy in India have mostly been centred around gauging the views of enterprises.[8] For example, the National Science and Technology Management Information System[9] under the Department of Science and Technology conducts periodic national surveys to collect data on resources dedicated to research and development (R&D) in science and technology (S&T). The data is collected from 6,000 tech R&D organisations including multinational corporations, non-government organisations, educational institutions, and private and public sector enterprises across India. The data informs India's score on national R&D indicators for assessment and policy formulation.

Meanwhile, McKinsey Global Institute in March 2019, surveyed more than 600 private enterprises and conducted interviews with stakeholders from the government and civil society. The survey was part of an ongoing series that tracks the impact of digital technologies on regions around the world, including India,[10] the United States, and Europe. In the context of India, the study aimed to map how digital capabilities could assist in increasing productivity and reshaping business value chains, and enhance the economic prosperity of Indian citizens. The focus was on four sectors that could benefit immensely from digitisation: agriculture, healthcare, logistics, and retail.

[8] Nirvikar Singh, "Information Technology and its Role in India's Economic Development: A Review", *UCSC*, (2014), https://economics.ucsc.edu/research/downloads/Singh_Paper_IGIDR25th_2014.pdf.

[9] Department of Science and Technology, "National Science and Technology Management Information System'', Ministry of Science and Technology, http://nationalsandtsurvey.nstmis-dst.org.

[10] Noshir Kaka et al., Digital India - Technology to Transform a Connected Nation, Mckinsey Global Institute, 2019,https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20India%20Technology%20to%20transform%20a%20connected%20nation/MGI-Digital-India-Report-April-2019.pdf.

While enterprises provide critical insights into the development side of technology, citizens are better placed to provide views on the impacts of these technologies on society. Yet, surveys that measure technology policy awareness of Indian citizens have been few and far between. One of the first detailed investigations on the Indian youth's awareness of privacy issues was conducted in late 2012 by researchers from the Indraprastha Institute of Information Technology in Delhi. It had 10,427 respondents and also included focus group discussions and expert interviews.[11]

As the adoption of technological innovations soared in recent years, especially during the first waves of the COVID-19 pandemic, there has been an increase in citizen-centric surveys that examine the impacts of these technological advancements. These include initiatives by the *Washington Post* and the Schar School of Policy and Government at George Mason University in November 2021;[12] the Pew Research Center survey, "The Future of Digital Spaces and Their Roles in Democracy"; and Elon University's 'Imagining the Internet Centre', also in November 2021.[13] The European Commission released its *Special Eurobarometer Report - Digital Rights and Principles*[14] in December 2021, which was based on a survey that gauged the views of EU citizens on the role of digital tools in their lives, their perception about online rights, and the proposed European common principles on digitalisation. In February 2021, Ernst

[11] Ponnurangam Kumaraguru and Niharika Sachdeva, "Privacy in India: Attitudes and Awareness V 2.0", *Indraprastha Institute of Information Technology,* Delhi, (2012), https://precog.iiitd.edu.in/research/privacyindia/PI_2012_Complete_Report.pdf.

[12] The Washington Post and Schar School of Policy and Government, "Washington Post-Schar Poll," 2021, https://www.washingtonpost.com/context/nov-4-22-2021-washington-post-schar-school-tech-poll/1f827037-688f-4030-a3e4-67464014a846/?itid=lk_inline_manual_6.

[13] Janna Anderson and Lee Rainie, *The Future of Digital Spaces and Their Role in Democracy,* Pew Research Centre, 2021, https://www.pewresearch.org/internet/2021/11/22/the-future-of-digital-spaces-and-their-role-in-democracy/.

[14] European Commission, *Digital Rights and Principles,* 2021,https://europa.eu/eurobarometer/surveys/detail/2270.

and Young (EY), under its Connected Citizens Programme, conducted a global survey[15] to assess people's views on how technology is shaping their lives.

In India, the Office of Principal Scientific Advisor of the Prime Minister and the IIT Madras Alumni Association conducted a survey in November–December 2020.[16] It covered 1,564 respondents, and sought to gather insights on the attitudes of citizens towards the role played by S&T and emerging technologies in the pandemic-era 'new normal' of work and economic opportunities Meanwhile, CUTS International, a think tank based in India conducted a survey[17] in March 2021 to measure consumers' understanding of policies on encryption.

While these surveys may have provided answers to the questions outlined in their research design, they failed to accord focus on India's youth—the country's so-called "demographic dividend". This is a gap that needs to be filled, as it is the youth who would have to live with the greatest impacts of the policies emanating from these discussions.

ORF's technology policy survey, *Swiping Right on Tech Policy,* was administered from October to November 2021 to 2,002 Indians aged 18 to 35. The aim was to bridge the gap in youth's voices in deliberations around technology policy, especially at the intersection of individual privacy, national sovereignty and security, and economic well-being.

[15] Arnauld Bertrand and Julie McQueen, *How can digital government connect citizens without leaving the disconnected behind?,* Ernst and Young, 2021, https://www.ey.com/en_gl/government-public-sector/how-can-digital-government-connect-citizens-without-leaving-the-disconnected-behind.

[16] Office of the Principal Scientific Adviser to the Government of India and IIT Madras Alumni Association. *Science and Technology in the New Normal in India - A Public Attitude Study,* 2021, https://www.indiascienceandtechnology.gov.in/stihighlights/sti-era-new-normal-—-survey-report.

[17] Amol Kulkarni, Sidharth Narayan, and Setu Bandh Upadhyay, *Understanding Consumers Perspective on Encryption in India,* CUTS International, 2021, https://cuts-ccier.org/pdf/survey-finding-understanding-consumers-perspective-on-encryption.pdf.

Discussions on individual privacy cannot be done in isolation from the evolving political and economic environment wherein data-sharing is central to realising values such as national sovereignty and economic well-being. Analysts have often referred to the so-called "digital trilemma"[18,19]— between individual privacy, national sovereignty and security, and economic well-being.

This survey report investigates whether India's youth consider this trilemma. In the context of this survey, the digital trilemma, or the Penrose triangle, translates into individuals knowingly or unknowingly giving more importance to, or favouring two of these concerns while sacrificing the third. The report finds evidence in favour of such a tendency. In the post-pandemic world, there is a need to strive for a policy environment that accords equal importance to all three and reconciles them.

[18] Samir Saran, "Navigating the Digital 'Trilemma", *Observer Research Foundation,* (2016), https://www.orfonline.org/expert-speak/navigating-the-digital-trilemma-2/.

[19] Zsófia Hajnal, "The Impossible Trinity of Security, Freedom and Privacy", *Securitologia,* (2017), https://www.researchgate.net/publication/329337244_The_Impossible_Trinity_of_Security_Freedom_and_Privacy.

NOTES ON THE SURVEY

A. Structure of the Questionnaire

ORF, in collaboration with Impetus Research, administered the questionnaire to a sample set of 2,002 individuals, scattered across India's 36 states and union territories (UTs). The questionnaire was divided into four sections: demographic details; awareness of technology-related issues; perceptions on critical questions about technology; and inputs on relevant interventions that could determine future policies by the government and private sector (see Annexure for the questionnaire). The questions in sections two, three, and four belonged to one of three parameters: individual privacy, national sovereignty and security, and economic well-being.[20]

For the purposes of this survey, the term *individual privacy*[21] refers to the right to keep their personal and sensitive information (including biometrics, and financial and locational data) safe from unauthorised, non-consensual use by business and government entities. The scope of individual privacy as a concept covers

[20] The categorisation of questions with the three parameters is based on the authors' assessment of the level of relevance of each question vis-a-vis each parameter. For example, the question about data localisation could be assessed on all the three parameters. However, in the authors' judgement, it is most relevant to the parameter of 'individual privacy' and has been categorised as such.

[21] IAPP, "What is Privacy?" https://iapp.org/about/what-is-privacy/.

practices adopted by individuals to ensure cyber hygiene, and their understanding of consent framework and data localisation.

Security, meanwhile, is required for any community and is primarily a responsibility of the state.[22] Under *national sovereignty and security,* the survey studies the willingness of an individual to share their data with the government or private sector enterprises to ensure the country's sovereignty and law enforcement, along with their inclination to support technology protectionism and international collaboration for security purposes. Under *economic well-being*, the survey evaluates the willingness of individuals to share their data for better delivery of public services and economic gains, along with concerns around existing models of data-sharing.

As noted in the Non-Personal Data Governance Framework (NPDGF)[23] report by the Kris Gopalakrishnan Committee set up by the Ministry of Electronics and Information Technology (MeitY) in 2020, "From an economic lens, data is non-rivalrous, yet excludable, and its use could have both positive and negative externalities." The value of data is not necessarily accrued by individuals who are generating it or national jurisdictions within which it is generated, but by enterprises who are exercising control over it. In recent years, MeitY and NITI Aayog[24] have shared proposals with citizens as part of public consultations to ensure the value generated from data is distributed among citizens and society. This survey also included questions on novel models of data-sharing.

[22] David Baldwin, "The concept of security". *Review of International Studies.* Vol. 23, (1997), https://www.jstor.org/stable/20097464.

[23] MeiTy, *Report by the Committee of Experts on Non-Personal Data Governance Framework,* July 2020; https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf; December 2020 https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf.

[24] NITI Aayog, Government of India, *Data Empowerment and Protection Architecture,* (August 2020). https://www.niti.gov.in/sites/default/files/2020-09/DEPA-Book.pdf.

B. Survey Design

The respondents belonged to the age group of 18 to 35 years. The survey was conducted by telephone—considering the constraints of the COVID-19 pandemic—and covered 2,002 Indian citizens residing in urban districts. The survey employed a stratified population sampling technique to arrive at a representative sample, with "representativeness" being defined in relation to the objectives of the study. Since the sample consisted only of mobile-phone users, it was stratified by telecom circles, resulting in 23 independent strata representing 36 states and UTs. Within each stratum, a random sample was drawn through Random Digit Dialling (RDD).

C. Accessibility and Inclusion

The survey questions were framed in a manner accessible to a wide base of respondents, and care was taken in the use of complex terminology or jargon. Moreover, to ensure the integrity of the survey, the questionnaire was translated into regional languages. The five-point Likert scale[25] was employed in the formulation of the questionnaire. In alignment with other technology policy surveys and to account for the significant gap in digital literacy in India,[26] the questionnaire provided response options such as 'Refuse to answer' and 'Don't know'. As the survey was completely telephonic, it is characterised by limitations typically associated with such surveys. For example, non-verbal clues from the respondents would not have been captured by the survey data.

[25] Likert scale is a psychometric scale used in questionnaires for scaling responses.

[26] Sumeysh Srivastava, "International Literacy Day: Bridging India's Digital Divide", *Bloomberg*, September 8, 2020, https://www.bloombergquint.com/technology/international-literacy-day-bridging-indias-digital-divide.

D. Methodology for Analysis

The survey aimed to shine a light on the perceptions of India's youth on issues related to the country's technology policy. The analysis uses an appropriate combination of descriptive statistics and statistical inference to tease out certain patterns in the respondents' views. The authors have used the basic tool of 'percentages' and 'proportions'—more specifically, percentage or proportion of responses, that end up being the core statistical entities anchoring the primary statistical investigations that were undertaken.

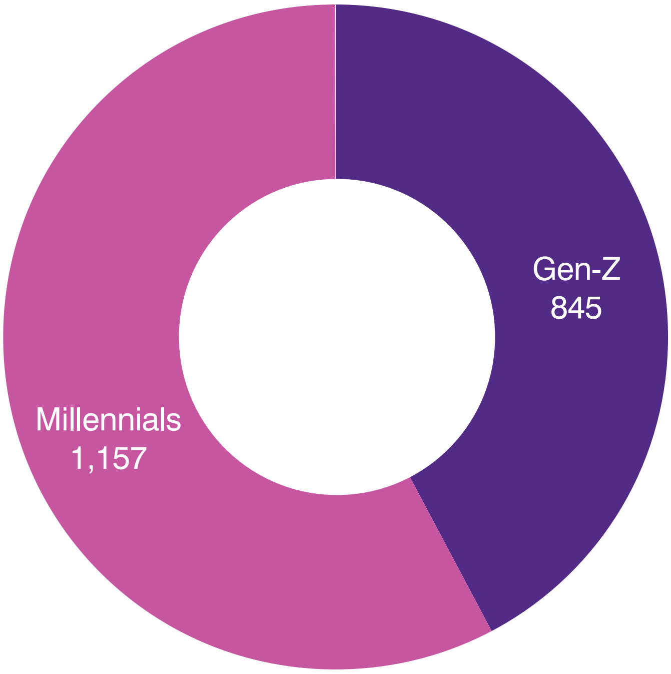
The authors have aggregated certain responses for purposes of the analysis. For example, the responses of 'always' and 'very often' have been combined into 'often'; the responses of 'very comfortable' and 'somewhat comfortable' have been combined into 'comfortable'; the responses of 'very important' and 'somewhat important' have been combined into 'important'; the responses of 'strongly agree' and 'somewhat agree' have been combined into 'agree'; and the responses of 'strongly support' and 'somewhat support' have been combined into 'support'. Furthermore, the percentage values shown in the pie charts may not add up to an exact 100 percent in all instances as the percentages are rounded off decimal numbers. Nevertheless, they will always be close to 100 percent.

This study gauges the predominant mood of those surveyed, while providing important insights on any remarkable deviations across the responses. These variances could belong to different categories of important demographic variables such as age, gender, geography, education, and occupation. To discern whether the difference in the percentage of responses across categories of demographic factors are statistically significant, the authors employ the test of significance for different proportions in large samples.

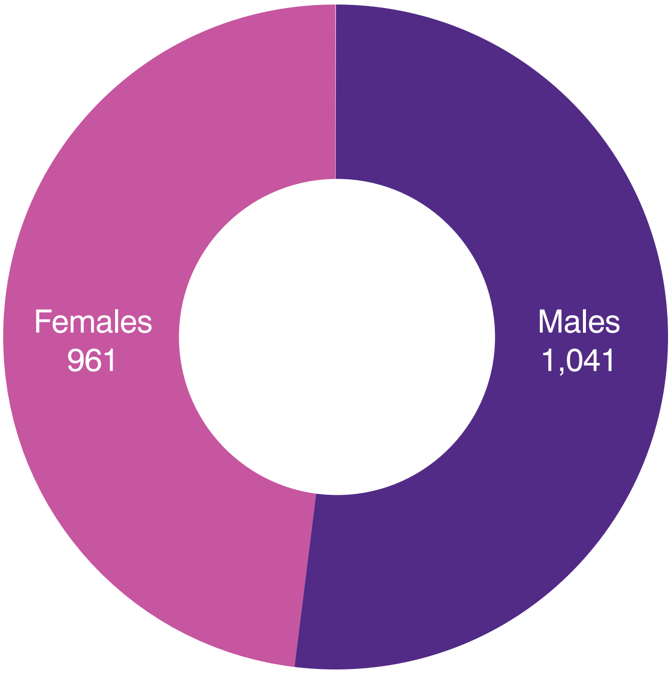
The survey set out with the hypothesis that a digital trilemma or a Penrose triangle exists between the values of individual privacy, national sovereignty and security, and economic well-being. The investigation is anchored in the notion of ‘proportion of responses’. However, in one part of this investigation, this proportion is calculated in a different manner to suit the requirements of the analysis. (The complete methodology is discussed in detail in a latter section of this report.)

The variables are defined as follows:

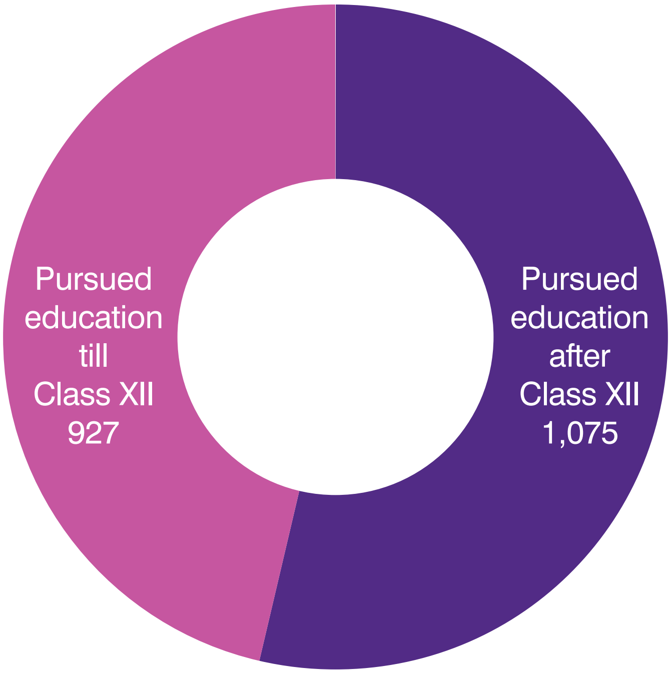
Distribution by Age: Gen-Z, which covers those born between 1995 and 2004; and Millennials, or those born between 1987 and 1994



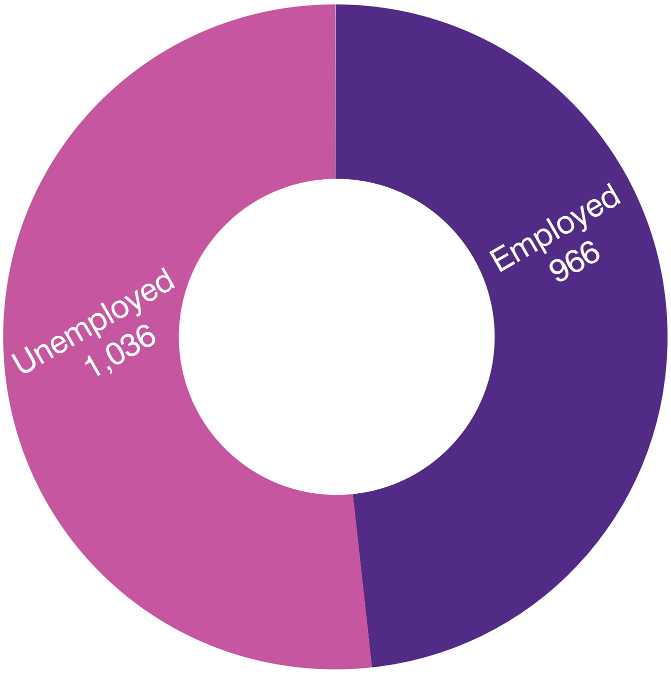
Distribution by Gender: Males and Females



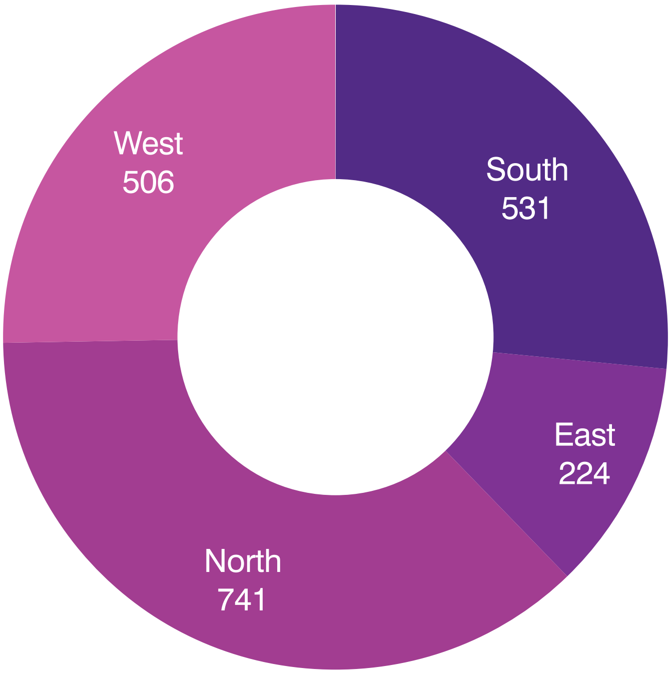
Distribution by Education: Those who pursued education after school, including those who have completed or are enrolled for their diplomas, undergraduate and postgraduate degrees; and those who studied till class XII or below.



Distribution by Occupation Status: Employed and Unemployed



Distribution by Geographical Region: North, South, East, and West[27]



[27] In this study, South includes Andhra Pradesh, Telangana, Karnataka, Kerala, Tamil Nadu, Lakshadweep and Chennai; North consists of Delhi, Western Uttar Pradesh, Eastern Uttar Pradesh, Haryana, Himachal Pradesh, Jammu and Kashmir, Punjab, Rajasthan, Bihar and Jharkhand, Madhya Pradesh and Chattisgarh; West is composed of Gujarat, Maharashtra, Goa and Mumbai; and East comprises Assam, Kolkata, North East, West Bengal and Odisha. Despite being cities, Mumbai, Kolkata and Chennai have been considered separately from the states they belong to, given their distinct importance in the telecom circle.

FINDINGS AND ANALYSIS

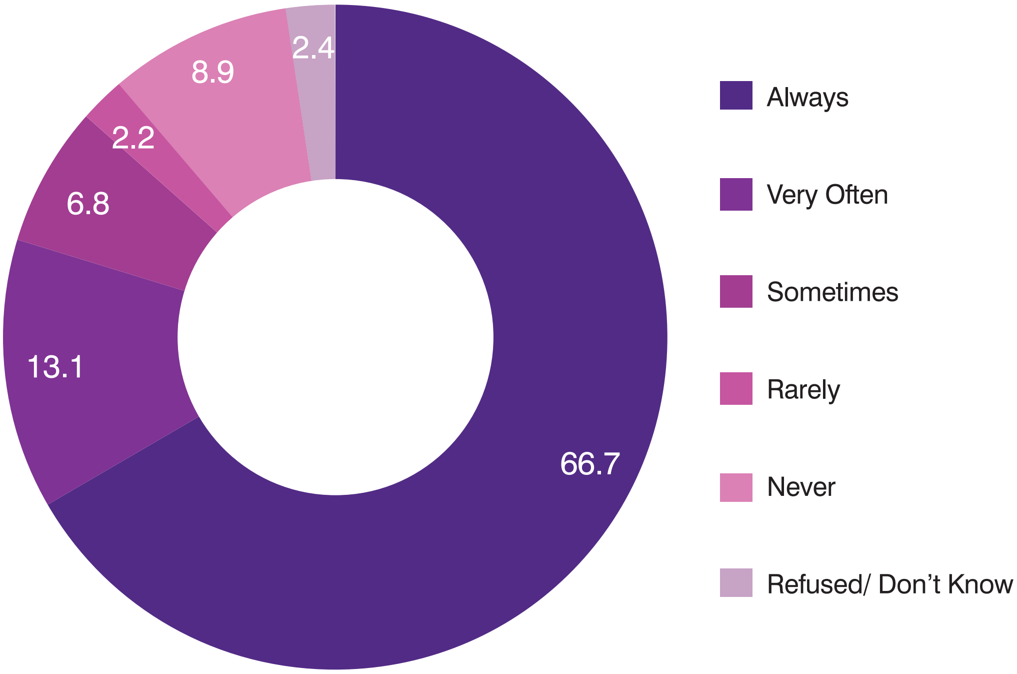
A. Individual privacy

a) Cyber-hygiene practices

Cyber-hygiene practices include activities that respondents engage in to keep their data private and safe. The survey posed questions on how often respondents practise cyber hygiene: keeping strong passwords; having different passwords for different accounts and keeping them confidential; clearing browsing history; reading privacy policy before registering on applications; updating software and using privacy settings on social media to restrict access to personal information. More sophisticated measures include the use of virtual private network (VPN); enabling two-factor authentication on devices; and allowing limited access to sensitive data like photos, location, and contacts to a new application that is downloaded on the phone.

The survey found between 60–80 percent of respondents practising staple measures, and a lower 24–57 percent practising sophisticated cyber hygiene. The staple cyber hygiene measure followed by the highest percentage of respondents (80 percent) is keeping passwords confidential, while that which receives the lowest attention (59.2 percent) is reading the privacy policy before registering on an application—predictably, perhaps, since the act of reading privacy policies takes time[28] and requires an understanding of legal jargon.[29]

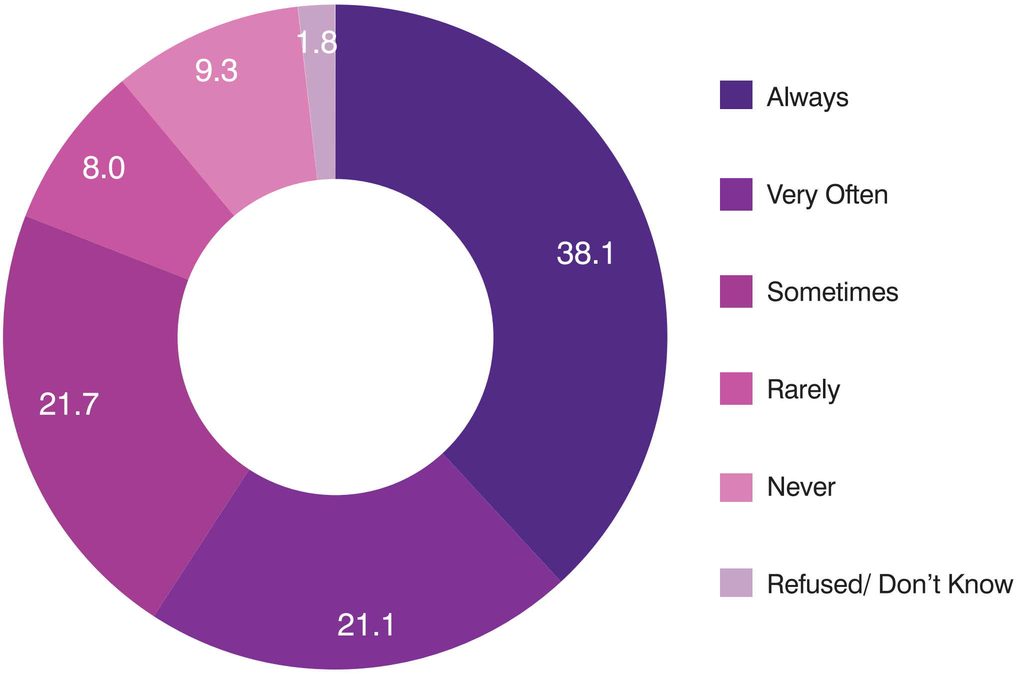
How often do you keep your passwords confidential?



[28] Aleecia M. McDonald and Lorrie Faith Cranor. "The Cost of Reading Privacy Policies". *I/S: A Journal of Law and Policy for the Information Society.* 2008 Privacy Year in Review Issue. (2008) https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

[29] Varad Pande and Subhashish Bhadra, "Privacy policies online are illegible and 'consent' is broken. New ideas are needed" *The Indian Express,* January 18, 2021, https://indianexpress.com/article/opinion/columns/privacy-policy-online-consent-illegible-7150434/.

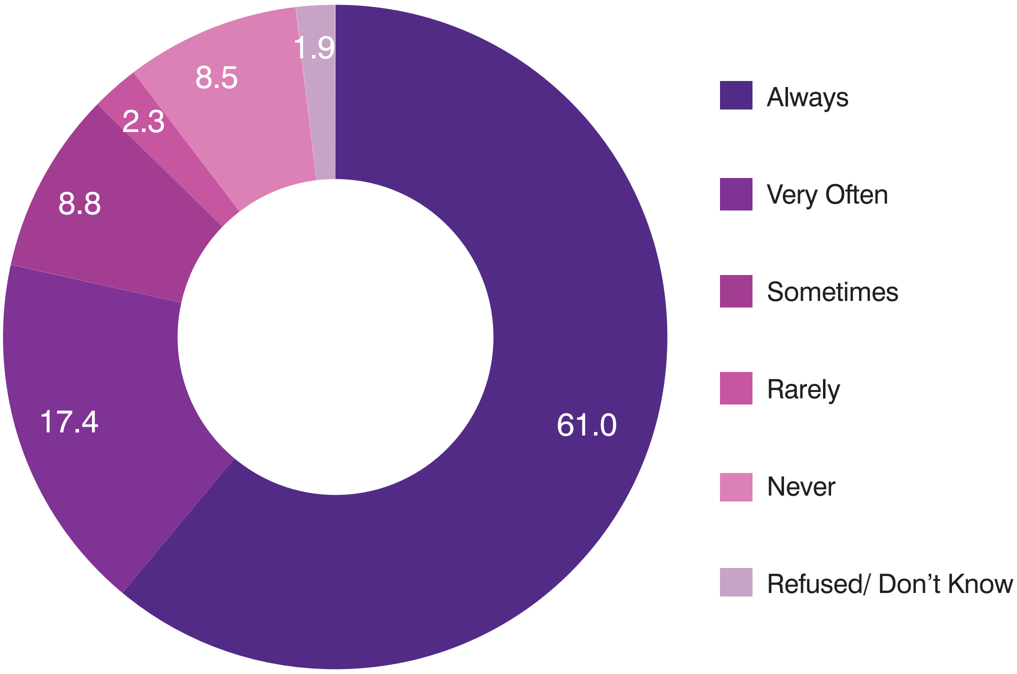
How often do you read the privacy policy before registering on any application?



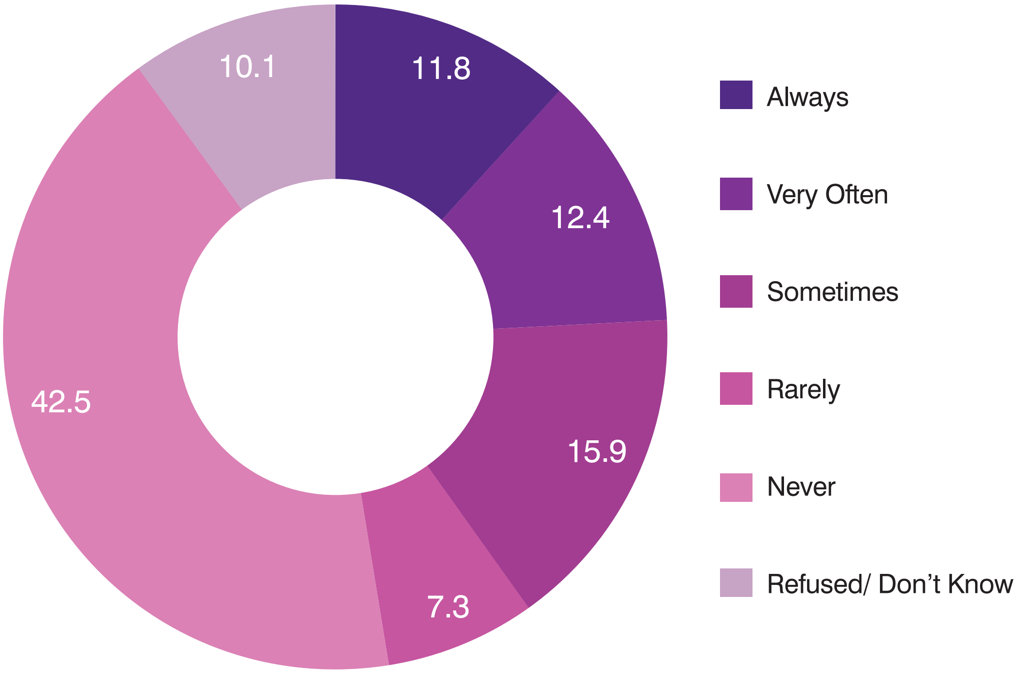
Among the regions, East India is the top performer in most of the staple data hygiene practices. For instance, a majority (from 66 to 86 percent) of the respondents from East India follow staple cyber-hygiene practices, of which the most popular measure is keeping strong passwords. South India, meanwhile, takes the lead in the more sophisticated cyber hygiene measures, with 39–53 percent of the respondents following such practices often. This can partly be explained perhaps by the existence of major IT hubs like Bengaluru[30] in the region and the assumed tech-savviness of respondents. Of the 531 respondents from South India, 38.6 percent use a VPN (as compared to East India, for example, where a lower 20 percent of the respondents do so). Using the test of significance for difference of proportions in large samples, the deviation between South India and East India in using VPN is statistically significant at the five-percent level of significance.

[30] Sanjeev Sinha, "Bengaluru ranked as one of the Top 5 technology centres in Asia Pacific". Financial Express, June 22, 2021, https://www.financialexpress.com/money/bengaluru-ranked-as-one-of-the-top-5-technology-centers-in-asia-pacific/2276088/.

How often do you keep strong passwords with uppercase letters, lowercase letters, numbers and special characters?



How often do you use a VPN?



Within South India, 37.1 percent of those currently employed at the time of the survey, use VPN; the proportion for those unemployed is 34.5 percent. This divergence, however, is statistically insignificant at the five-percent level of significance.[31] Similarly, within South India, 42.7 percent of those with a higher degree of education use VPN, while 28.6 percent of the respondents with a lower degree of education do. Here, the divergence is statistically significant at the five-percent level of significance,[32] indicating that the degree of education positively impacts the practice of sophisticated cyber hygiene.

The survey found a higher proportion of male respondents practising both staple and sophisticated cyber hygiene measures compared to the females. For example, when asked whether they keep their passwords confidential, 70 percent of males said they did, *always* or *very often;* the proportion for the female respondents was a lower 63 percent. In the context of this question, the difference between the two proportions is statistically significant at the five-percent level of significance.[33] Indeed, various studies in India have found that young females tend to have a lower degree of digital awareness.[34, 35]

Another reason that could explain the gender-based divergence in responses to the question of keeping passwords confidential is that females, out of cautiousness on matters concerning the use of digital services like net banking and social media, may often share their passwords with male members of their family to seek their assistance.

[31] Results of the test of significance for difference of proportions in large samples: Z score = 0.5873, p-value = 0.5552

[32] Results of the test of significance for difference of proportions in large samples: Z score = 3.3922, p-value = 0.0007

[33] Results of the test of significance for difference of proportions in large samples: Z score = 3.3187, p-value = 0.0009

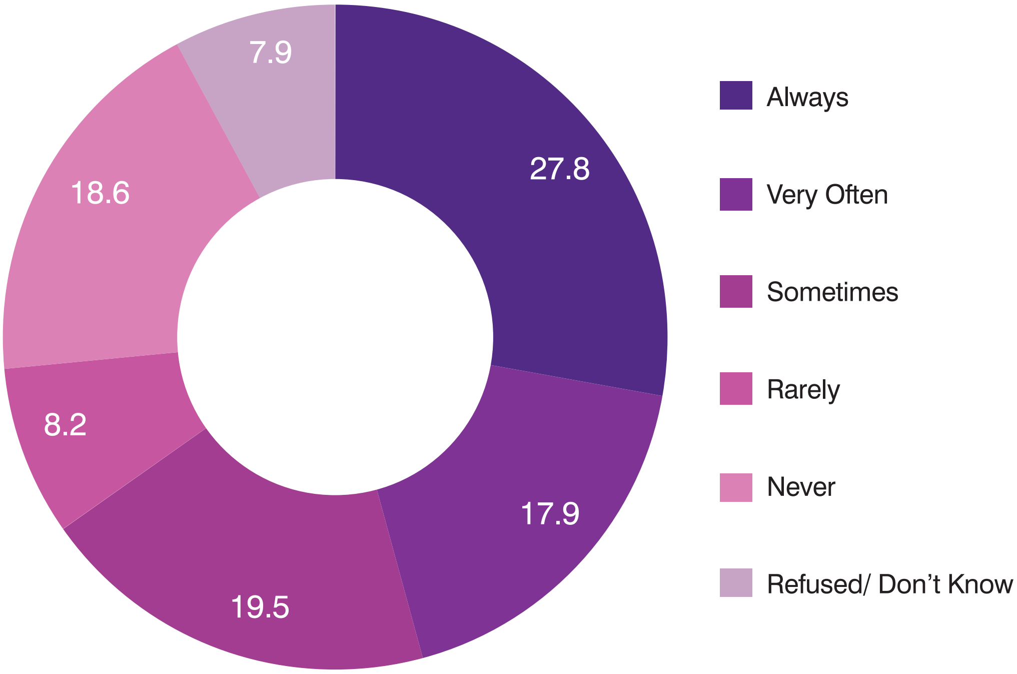
[34] "Digital Gender Gap Scorecard: India", (2017), https://1e8q3q16vyc81g8l3h3md6q5f5e-wpengine.netdna-ssl.com/wp-content/uploads/2017/01/A4AI-presentation.pdf.

[35] Simon Kemp, Digital 2021: India, Data Reportal, 2021, https://datareportal.com/reports/digital-2021-india.

They could also be obligated by their family members to share their passwords and use shared phones.[36]

To be sure, there are existing state-led digital literacy programmes such as the National Digital Literacy Mission, which purport to bridge the gaps in digital know-how. However, they have failed to effectively enhance digital awareness, largely due to a paucity of funds that could otherwise help them make their course material more dynamic amidst rapid changes in technology.[37] In other cyber hygiene measures, such as enabling two-factor authentication on their devices, and reading the privacy policy before registering on an application, the female and male respondents behaved similarly. Age-wise, Gen-Z respondents and their millennial counterparts are also on similar lines in terms of cyber hygiene. The deviations were statistically insignificant at the five-percent level of significance.

How often do you enable two-level authentication on your devices?

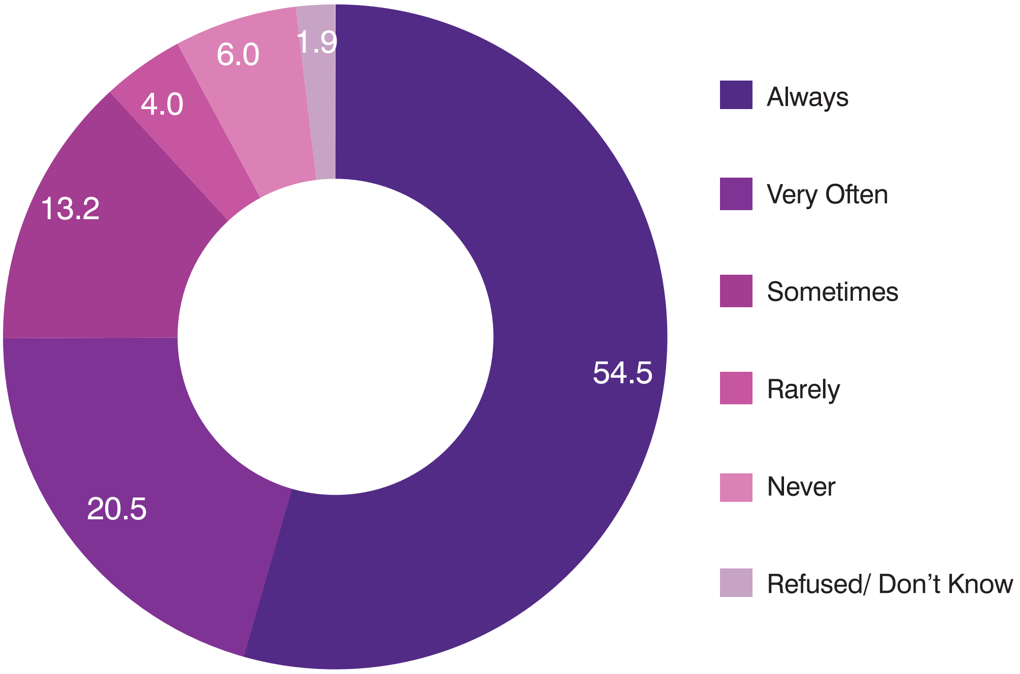


[36] Nithya Sambasivan and Garen Checkley, "Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia". (paper presented as part of the proceedings of the Fourteenth Symposium on Usable Privacy and Security.August 12–14, 2018 • Baltimore, MD, USA) https://www.usenix.org/conference/soups2018/presentation/sambasivan.

[37] Pavithra K M, "Review: Government's Digital Literacy targets not met because of paucity of funds". *Factly*, August 25, 2020, https://factly.in/review-governments-digital-literacy-targets-not-met-because-of-paucity-of-funds/.

The analysis finds that education positively impacts the practice of cyber hygiene. For example, 80.4 percent of the highly educated respondents kept software on their digital devices updated, while the proportion was a lower 68.5 percent for those with lower levels of education. This divergence across education levels is particularly prominent in the practice of more sophisticated cyber hygiene measures.

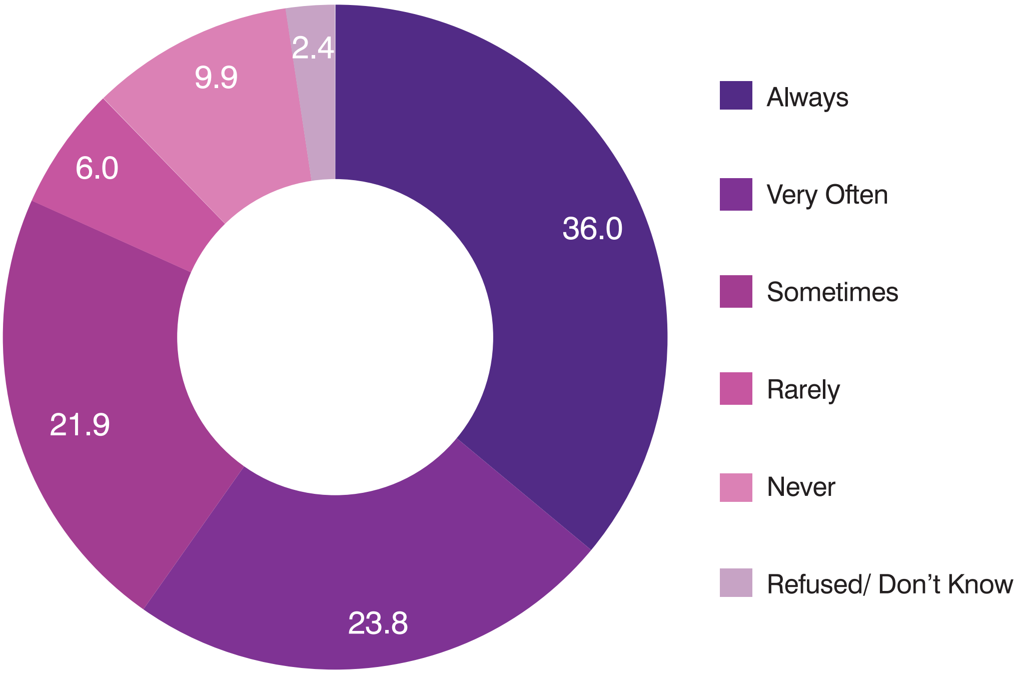
How often do you update your software?



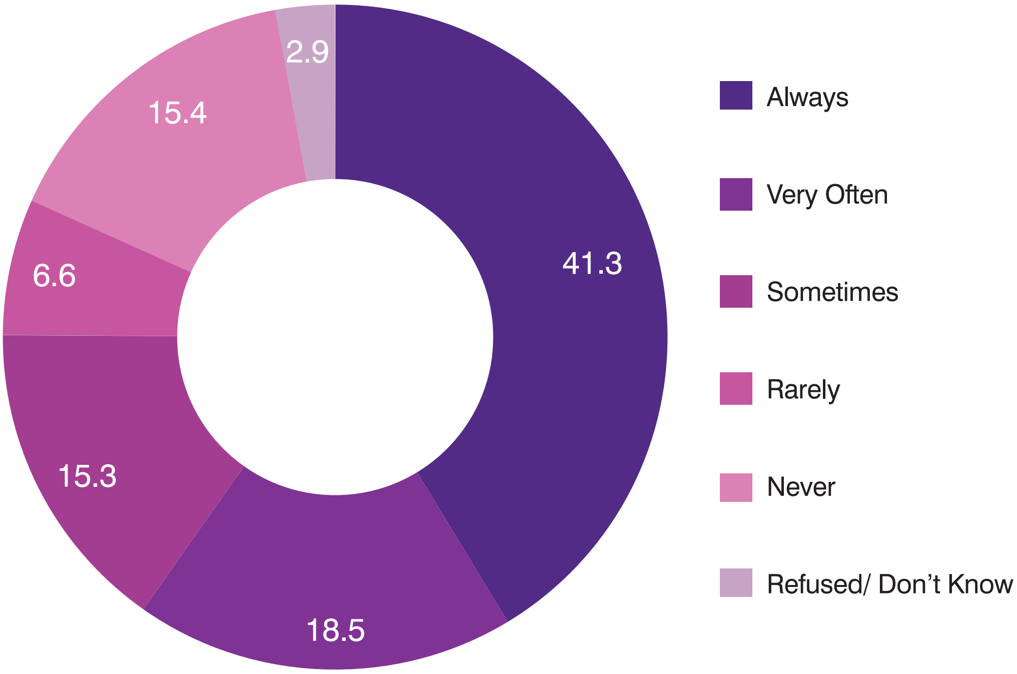
Respondents who are employed engage more consistently in both staple and sophisticated cyber-hygiene practices. For example, 83.5 percent of the employed respondents kept their passwords confidential, and 76.3 percent of the unemployed did so—this difference is statistically significant at the five-percent level of significance.[38] Perhaps the requirements of their job push employed respondents to hone skills required for maintaining official email and other accounts that store professional and sensitive information.

[38] Results of the test of significance for difference of proportions in large samples: Z score = 4.003, p-value is very close to zero

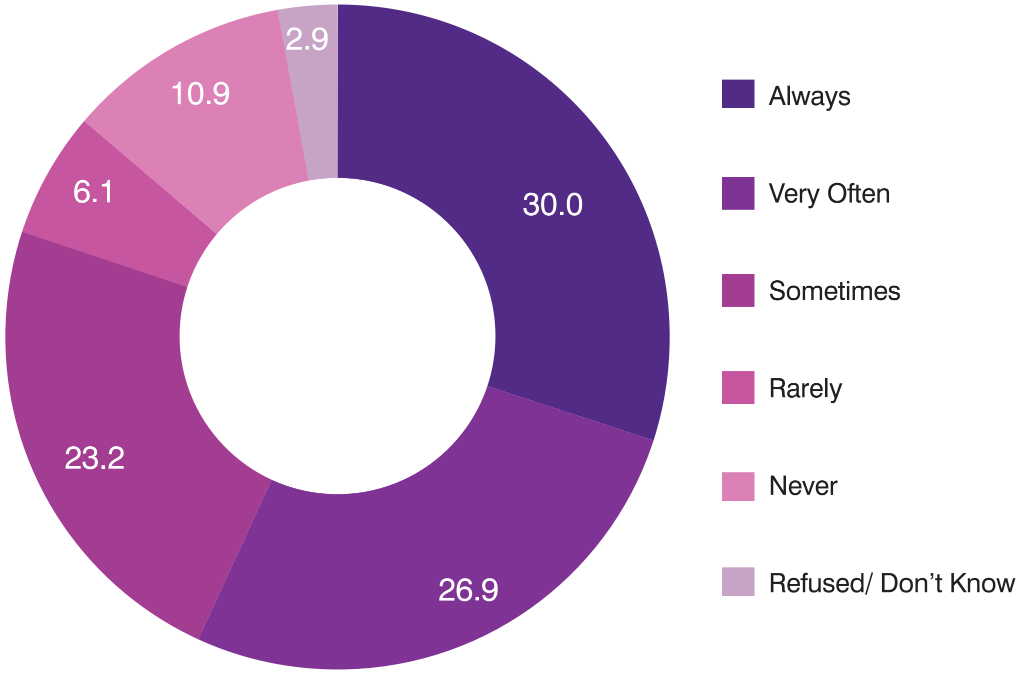
How often do you clear your browsing data?



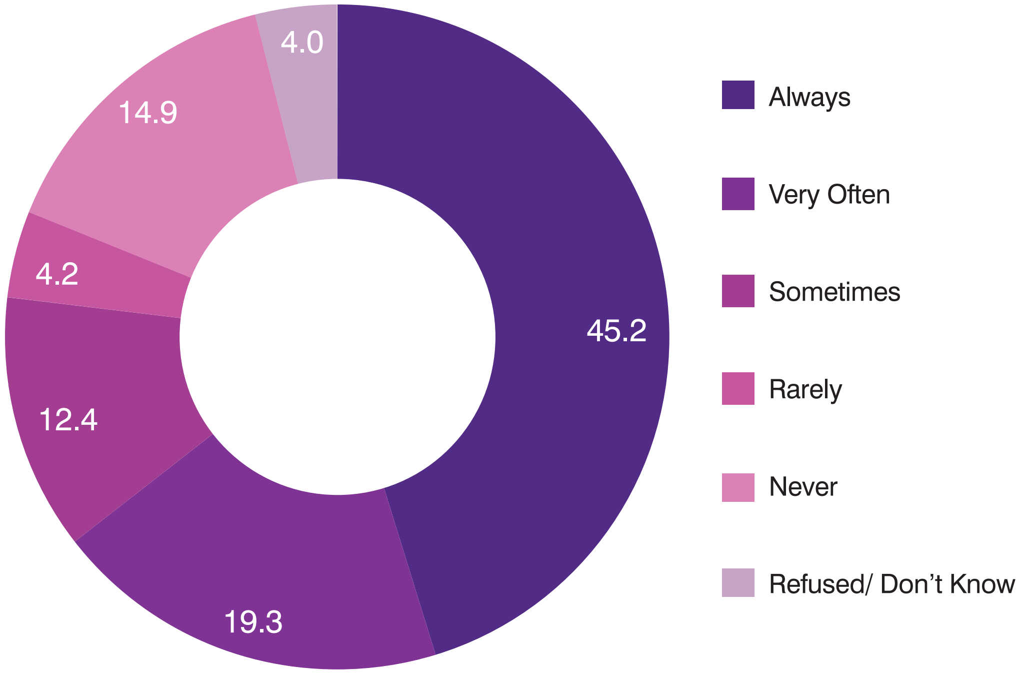
How often do you keep different passwords for different accounts?



How often do you allow limited access to sensitive data like photos, location, and contacts to a new application that you download on your phone?



How often do you use privacy settings on social media to restrict access to personal information?



b) Consent framework for data-sharing

The practise of securing consent from users for data sharing and ensuring privacy is mandated under Section 72 of the Information Technology Act 2000 (IT Act).[39] However, the Act does not stipulate the scope and definition of both 'consent' and 'privacy'. In 2017, MeitY released the Electronic Consent Framework, Technology Specifications Version 1.1[40] to provide a comprehensive technological framework for the effective implementation of existing policies on sharing data and securing electronic consent[41] from users. In the financial sector, the Reserve Bank of India (RBI) issued, in 2016, the Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions[42] to establish a consent architecture for consumers engaging in financial services. Meanwhile, in the health sector, the Ministry of Health and Family Welfare released the Health Data Management Policy in 2020[43] to establish a consent framework for processing personal health data; the policy was informed by the Personal Data Protection Bill, 2019.[44]

[39] Ministry of Law, Justice and Company Affairs, *Information Technology Act,* 2000 https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=.

[40] Ministry of Electronics and Information Technology, Electronic Consent Framework - *Technology Specifications, Version 1.1,* 2017, https://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf.

[41] Electronic consent allows sharing of digital data of users after informed consent has been sought electronically by the user in a secure manner.

[42] Reserve Bank of India, *Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions,* 2016, https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598.

[43] National Digital Health Mission, *Health Data Management Policy,* 2020, https://abdm.gov.in/documents/health_management_policy.

[44] Lok Sabha. *The Personal Data Protection Bill,* 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

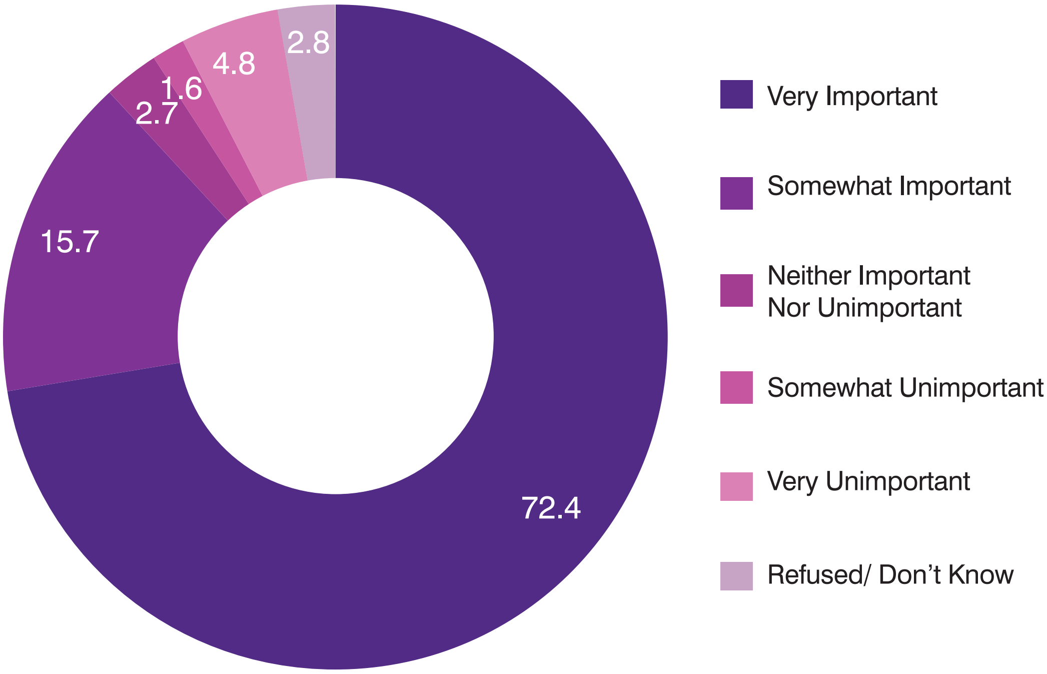
The Electronic Consent Framework is guided by five design principles:

1. User centricity: Users should have adequate decision-making power and control to restrict how data about them is being shared.
2. Trustable and compliant with IT Act: There should be a trail of digital signatures to satisfy the integrity of permissions granted by the user.
3. Universal identity: Universal and non-repudiable digital identities should be used to facilitate interoperability of data across service providers.
4. Granular control: Users should have control to restrict access to data at a granular level.
5. Open standards-based: The framework should utilise open technology and be agnostic to platforms, applications, and programming languages.

More than 80 percent of the respondents expressed support for the principles that underlie the functioning of the consent framework. More than eight of every 10 respondents (88.1 percent) consider user-centric mechanisms for data sharing as important and support the requirement that consent be sought before the commencement of data sharing. Overall, female and male respondents shared similar views (79.1 percent and 88 percent) across regions. Nevertheless, within South India, females (89 percent) support having a say in how data is shared between entities, more than males (83.2 percent). In the context of this question, the difference between the proportions is statistically significant at the five-percent level.[45]

[45] Results of the test of significance for difference of proportions in large samples: Z score = 3.7348, p-value = 0.0002

Do you think that you should have a say in how your data is shared — for instance, browsing data, transaction history, and profile held by institutions such as social media companies, banks, government departments, hospitals/doctors, and mobile apps?

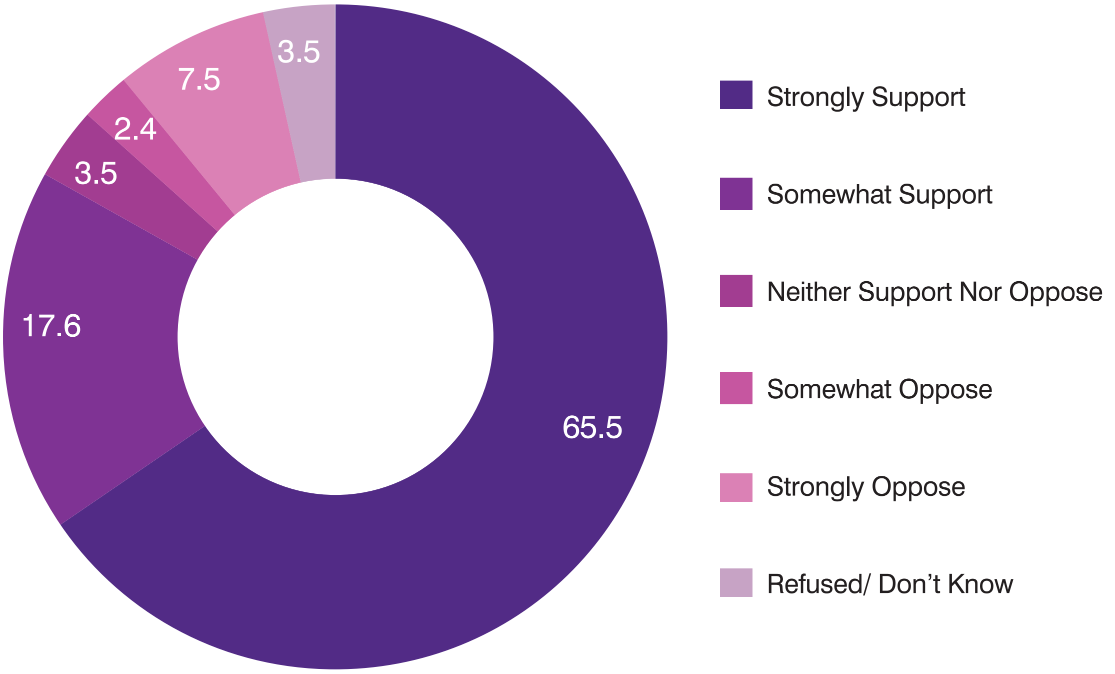


The survey found that age is not a significant factor in the understanding of, and agreement to consent frameworks on data sharing. Of the Gen-Z respondents, 81 to 88 percent support consent frameworks; among the millennials, the results were from 82 to 88 percent. Disaggregating the data by age and gender gives the same results: A significant majority of both Gen-Z and millennials across gender support the principle of determining how their data is shared.

Overall, 83 percent of all respondents support having granular control over their data to revoke consent and set limitations to data-sharing between companies. A substantial 89.3 percent of respondents in West India and 86.1 percent in East India agree that citizens should be able to set limitations on data usage and sharing between companies. The proportion is a lower 79.1 percent in South India. The

10.1 percent difference is statistically significant at the five-percent level of significance.[46] Given South Indian youth's steady professional involvement with technological corporations and other companies involved in data sharing, they perhaps have more trust in the data-sharing practices of private enterprises.

Do you support the ability of citizens to set limitations on data usage and sharing between companies?

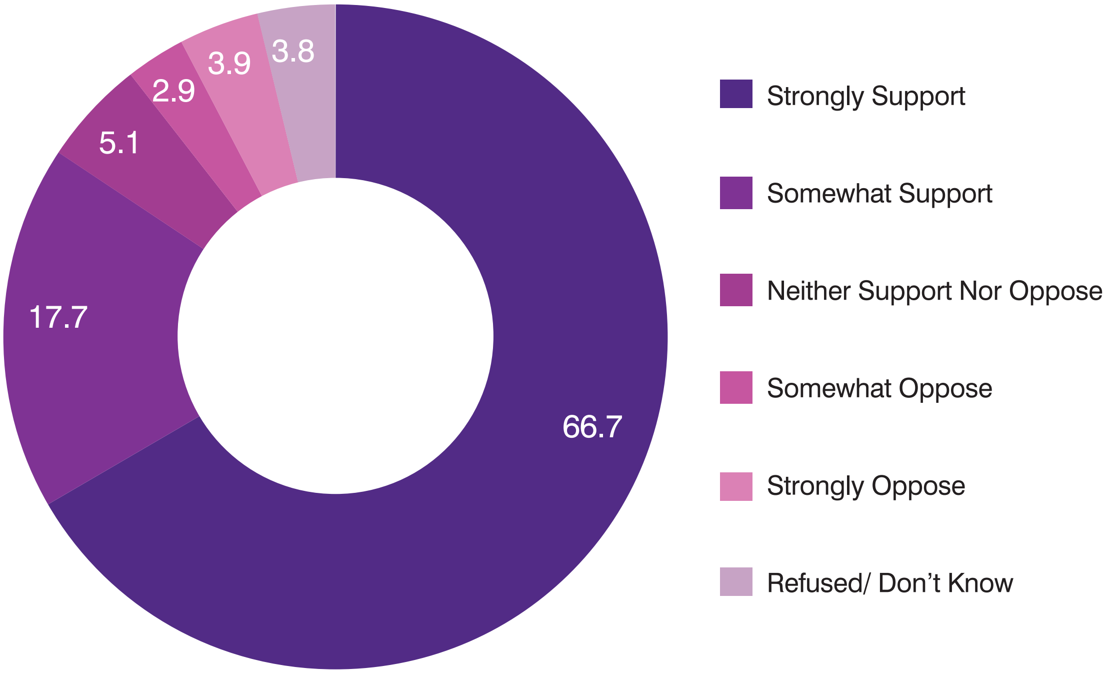


More than eight of every 10 respondents (84.4 percent) support institutionalising a centralised system with a unique ID and password for citizens to be able to verify and update information saved by the government about them. Of the respondents from West India, the proportion is 88.3 percent; for South India, it is 80.6 percent. The 7.7 percent difference is statistically significant

[46] Results of the test of significance for difference of proportions in large samples: Z score = 4.456, p-value is very close to zero

at the five-percent level of significance.[47] This could indicate a potential lack of trust among the youth of South India in the centralised, unique ID system. Indeed, in 2019, there was a massive Aadhaar data breach[48] that compromised the data of 1.1 billion registered Indian citizens.

Do you support institutionalising a centralised system with a unique ID and password for citizens to verify and update information that is being saved about them by the government?



[47] Results of the test of significance for difference of proportions in large samples: Z score = 3.412, p-value = 0.00064

[48] World Economic Forum, The Global Risks Report 2019 14th Edition, 2019, https://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.

About 83 percent of both employed, and also 83 percent of unemployed respondents support the principle of giving citizens the right to set limitations on data sharing between companies. Of those who are employed, 87.1 percent support institutionalising a centralised system; the proportion is 83.5 percent for the unemployed respondents. The 3.6 percent difference is statistically significant at the five-percent level of significance.[49]

Nearly eight of every 10 respondents (79 percent agreed with the mandatory erasure of a user's personal information on the request of the user, as well as information that was being collected and processed by private companies. The *right to data erasure* or *the right to be forgotten* has its roots in the European understanding of the principle of privacy. The EU's General Data Protection Regulation (GDPR)[50] requires data controllers[51] to remove users' inadequate and irrelevant personal data if they are unlawfully processed and consent has been withdrawn under Article 17 of the GDPR. While discussions in India about this right are still nascent, the Joint Parliamentary Committee's Report on the Personal Data Protection Bill, 2019 (JPC report)[52] tabled on 16 December 2021 contains provisions guaranteeing the right under Clause 9.

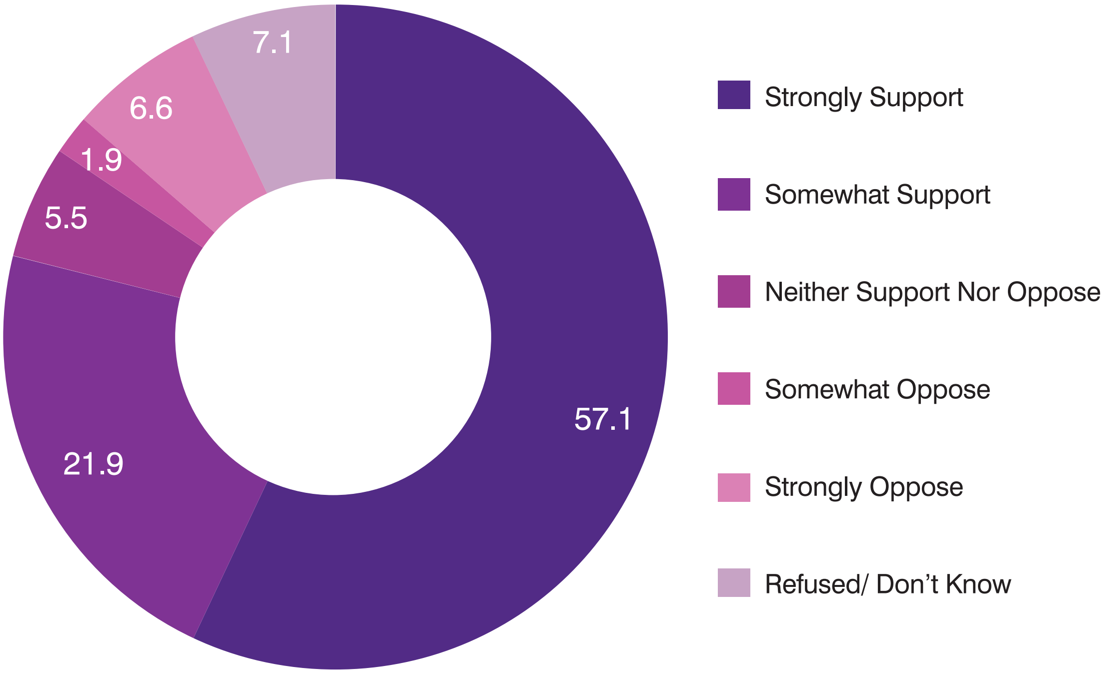
[49] Results of the test of significance for difference of proportions in large samples: Z = 2.268, p-value = 0.0117

[50] European Union, *General Data Protection Regulation*, 2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[51] Data controller is the entity responsible for collecting and processing data.

[52] Lok Sabha. *Report of the Joint Committee on The Personal Data Protection Bill,* 2019 (December 2021). https://www.ahlawatassociates.com/wp-content/uploads/2021/12/17-Joint-Committee-on-the-Personal-Data-Protection-Bill-2019.pdf.

Do you support mandatory erasure of user's personal information kept by private companies, on the request of the user?



The survey found a greater proportion of those who are highly educated (82.6 percent) supporting the right to be forgotten, compared to those with lower levels of education (74.8 percent). The divergence is statistically significant[53] and perhaps education level plays a role in the degree of awareness about such a right.

c) Data localisation

In early 2020, India banned Chinese social media platforms from operating in the country. In its statement, MeitY said the applications were "prejudicial to the sovereignty and

[53] Results of the test of significance for difference of proportions in large samples: Z score = 4.27, p-value is very close to zero

integrity of India, the defence of India, the security of state and public order."[54] China's National Intelligence Law of 2017[55] obligates all individuals and organisations (including tech companies) to provide the government data and intelligence they have collected, if needed for maintaining national security. By imposing the ban, the Government of India acknowledged that violations of data security and privacy often interfere with national sovereignty. Analysts have also observed that the ban was possibly a punitive measure on Chinese economic interests in response to the violent clashes between India and China at the Ladakh border in May 2020.[56]

The ban on Chinese platforms has led to a significant portion of the Indian population migrating to local apps.[57] Applications like Trell, Koo, and Chingari are today widely used across the country.[58] Additionally, MeitY, in collaboration with NITI Aayog, has been encouraging startups[59] to develop applications across sectors like social media, news, and gaming.

The survey found that 24.5 percent of the respondents often use local social networking sites over their foreign

[54] Ministry of Electronics and IT, "Government Blocks 118 Mobile Apps Which are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order", PIB, September 2, 2020, https://pib.gov.in/PressReleasePage.aspx?PRID=1650669.

[55] Standing Committee of the National People's Congress, Government of People's Republic of China, *National Intelligence Law of the People's Republic of China (2018 Amendment) [Effective],* 2018, https://en.pkulaw.cn/display.aspx?cgid=313975&lib=law.

[56] Karishma Mehrotra, "India bans 59 Chinese apps, including TikTok, ShareIt, UC Browser" Indian Express, June 29, 2020, https://indianexpress.com/article/india/china-apps-banned-in-india-6482079/.

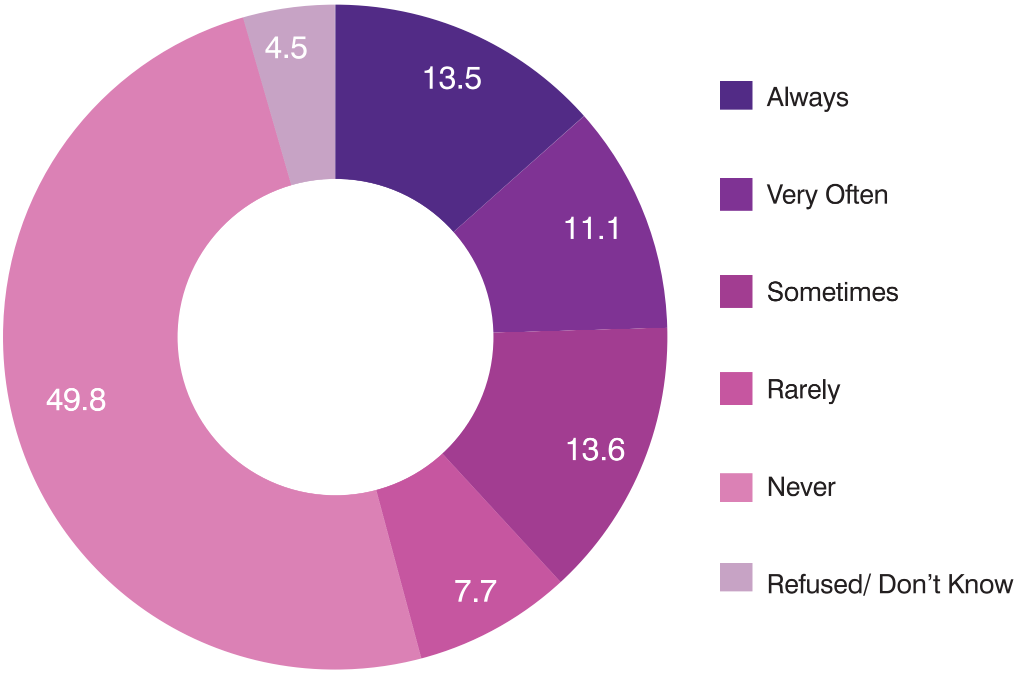
[57] Prasid Banerjee, "The race to build an Indian social network". *The Mint,* July 7, 2020, https://www.livemint.com/technology/apps/the-race-to-build-an-indian-social-network-11594043077273.html.

[58] "Social media platforms lead Social Commerce in India - Report", *Mint*, November 1, 2021, https://www.livemint.com/industry/retail/social-media-platforms-lead-social-commerce-in-india-report-11635758868407.html.

[59] Amrit Mohatsav App Innovation Challenge. https://innovateindia.mygov.in/app-innovation-challenge/; Digital India AatmaNirbhar Bharat Innovate Challenge. https://innovate.mygov.in/app-challenge/.

counterparts. Respondents from the Southern region have the highest preference for local social media platforms over foreign ones at 45.7 percent; the proportion is 17.5 percent for West India, 16.7 percent for North India, and 15.1 percent for East India. The 30.6-percent difference between the region with the highest proportion and that with the lowest—South and East India—is highly statistically significant at the five-percent level of significance. A plausible explanation is familiarity, as most Indian social media platforms such as Trell, Koo, and Chingari are based in the South. Overall, though, the preference for local platforms is low, at 21–27 percent; the

How often do you use Indian social media applications like Josh, Koo, Chingari and so on in comparison to foreign social media applications like Whatsapp, Twitter, Facebook, etc.?



trend is similar across gender, age, employment, and education. A little over 70 percent of the respondents stated their support for the Indian government's push for data localisation, or the storage and processing of personal data generated by Indians within the country's territory. Since 2016, RBI has already mandated the storage of all financial data of citizens within Indian borders.[60] The JPC Report of 2021 also proposed a data localisation framework under Clause 33 and 34. The government is of the view that data localisation is key to protecting critical information.[61]

Data localisation also assists in providing domestic law enforcement agencies with easy access to critical information when required. The push is stemming from the delay in obtaining data that can be used in investigations, stored in another jurisdiction and access to which is currently enabled through mutual legal assistance treaties.[62] Broken down by region, in West India, 77 percent of the respondents support data localisation; in South India, a lower 58.7 percent do so. The 18.3-percent difference is statistically significant at the five-percent level of significance.[63]

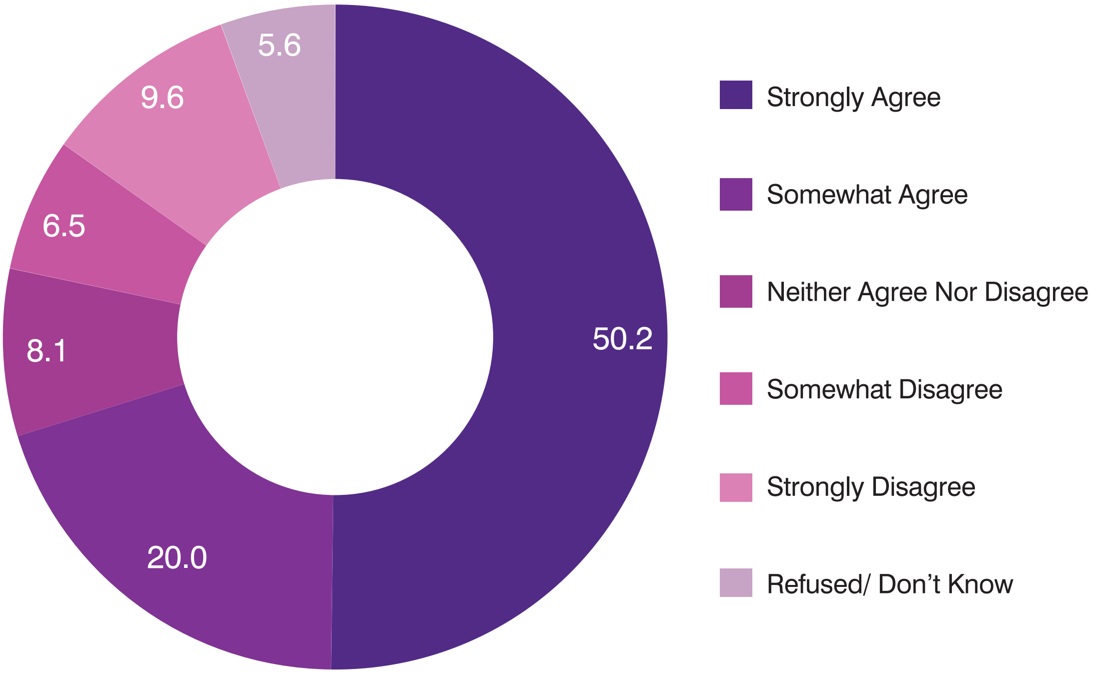
[60] Reserve Bank of India, *Storage of Payment System Data,* 2016, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244.

[61] The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 under Section 43A of Information Technology Act, 2000 is in force but to broaden the scope of responsibilities for stakeholders including businesses, the Draft Data Protection Bill 2021 was tabled in the Parliament in 2021.

[62] Anirudh Burman and Upasna Sharma, *How Would Data Localisation Benefit India?,* Carnegie India, 2021, https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291.

[63] Results of the test of significance for difference of proportions in large samples: Z score = 6.299, p-value is very close to zero

Should foreign tech firms localise storing and processing of data generated by Indian citizens?



Data localisation has more support from respondents with a higher level of education (74.1 percent), compared to those with lower levels of education (65.5 percent). The divergence is statistically significant at the five-percent level of significance.[64] Disaggregating responses simultaneously by education and region, the following is a breakdown in the proportions of those supporting data localisation: 81 percent of those with higher level of education from West India, 75.5 percent of those from East India, 74.8 percent from North India, and 63.5 percent from South India. Among those who studied till class XII or below, the following proportions of respondents support data localisation: 74 percent in East India, 72 percent in West India, 67.5 percent in North India, and 52.6 percent in South India. In the context of this question, divergences in the responses disaggregated by level of education are

[64] Results of the test of significance for difference of proportions in large samples: Z score = 4.192, p-value is very close to zero

statistically significant at the five-percent level of significance across North, South and West India; not in East India.[65]

Respondents across gender expressed equal support for data localisation. This trend is seen across different categories of age, as well as employment. Disaggregating responses simultaneously by employment and region, the survey found that more than 72 percent of the employed and unemployed in West, North, and East India support data localisation without differing significantly in their extent of support. Meanwhile, only 63 percent of the employed and 53 percent of the unemployed in South India support the proposition on data localisation. This difference in the responses due to employment status is statistically significant at the five-percent level.[66]

B. National Sovereignty and Security

a) Data sharing for national security and law enforcement

In 2017, the Supreme Court ruled that privacy is a fundamental right guaranteed under Articles 14,15,19 and 21 of the Indian Constitution, and like other fundamental rights, the right to privacy is not absolute.[67] Justice D. Y. Chandrachud, as part of the judgment, recommended that the government build a robust data protection regime that balances individual

[65] Results of the test of significance for difference of proportions in large samples:
North India : Z score = 2.1915, p-value = 0.02852
South India : Z score = 2.528, p-value = 0.0114
West India : Z score = 2.3808, p-value = 0.01732

[66] Results of the test of significance for difference of proportions in large samples: Z score = 2.3081, p-value = 0.02088

[67] Supreme Court of India, *Justice K.S.Puttaswamy(Retd) ... vs Union Of India And Ors.* Indian Kanoon, 2017, https://indiankanoon.org/doc/91938676/.

privacy and the legitimate concerns of the government.[68] The 2021 JPC report has fuelled concerns on state surveillance, with the addition of the words, "interest and security of the state" in its long title[69] under the Data Protection Bill 2021. Further, Clause 35 of the Bill empowers the Union government to exempt any government agency from the requirements of the Bill, if it is processing the personal data of a citizen for the legitimate concerns of the state. The US and Canada also have regulations that facilitate the sharing of information, including personal data, for national security purposes—in 2012, the US released the National Strategy for Information and Safeguarding;[70] and in 2019, Canada released the Security of Canada Information Disclosure Act.[71]

This present survey found that 59 percent of the respondents are comfortable sharing personal information such as medical records, locational data, and financial history to assist in law enforcement and for national security purposes. The results are remarkable for immediate needs like *ensuring road safety,* with 79 percent of the respondents saying they are comfortable sharing data to meet such purpose. Other long-term concerns and the proportion of respondents who are comfortable sharing data for them are: *reducing organised cybercrimes* (67.5 percent); *stopping foreign interference in domestic elections* (63 percent); and *supporting anti-terrorism efforts* (59 percent).

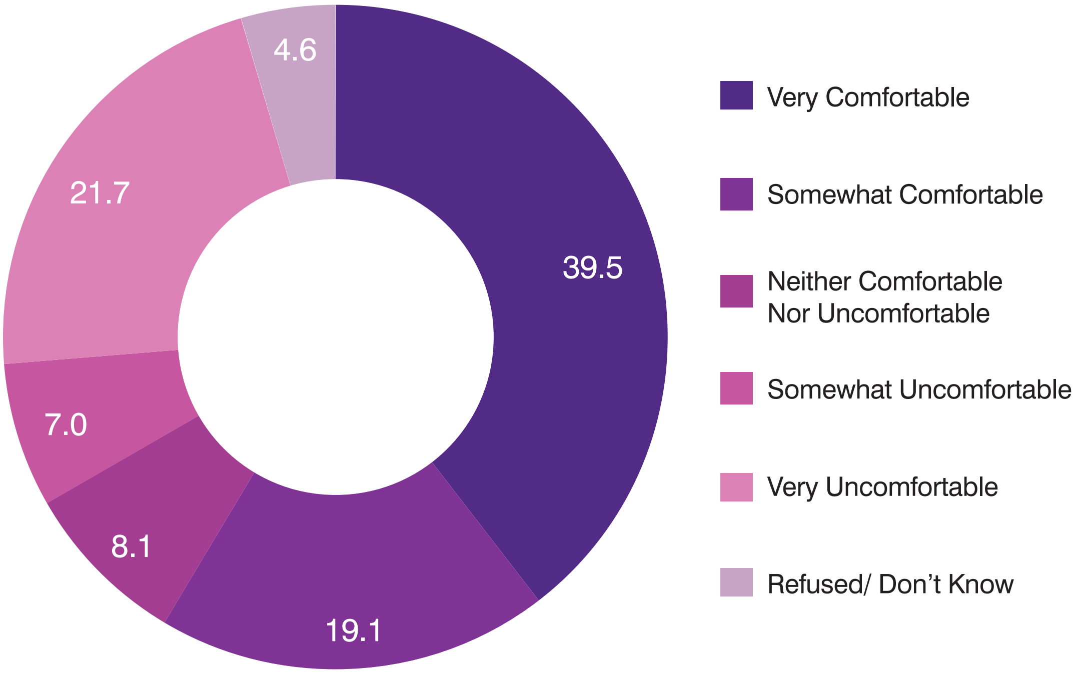
[68] PTI, "Privacy a protected right emerging from Article 21: Supreme Court," *Economic Times,* August 24, 2017, https://economictimes.indiatimes.com/news/politics-and-nation/privacy-a-protected-right-emerging-from-article-21-supreme-court/articleshow/60209881.cms?from=mdr.

[69] Apar Gupta and Vrinda Bhandari, "National security, at the cost of citizens' privacy," *Indian Express,* December 20, 2021, https://indianexpress.com/article/opinion/columns/national-security-at-the-cost-of-citizens-privacy-7680787/.

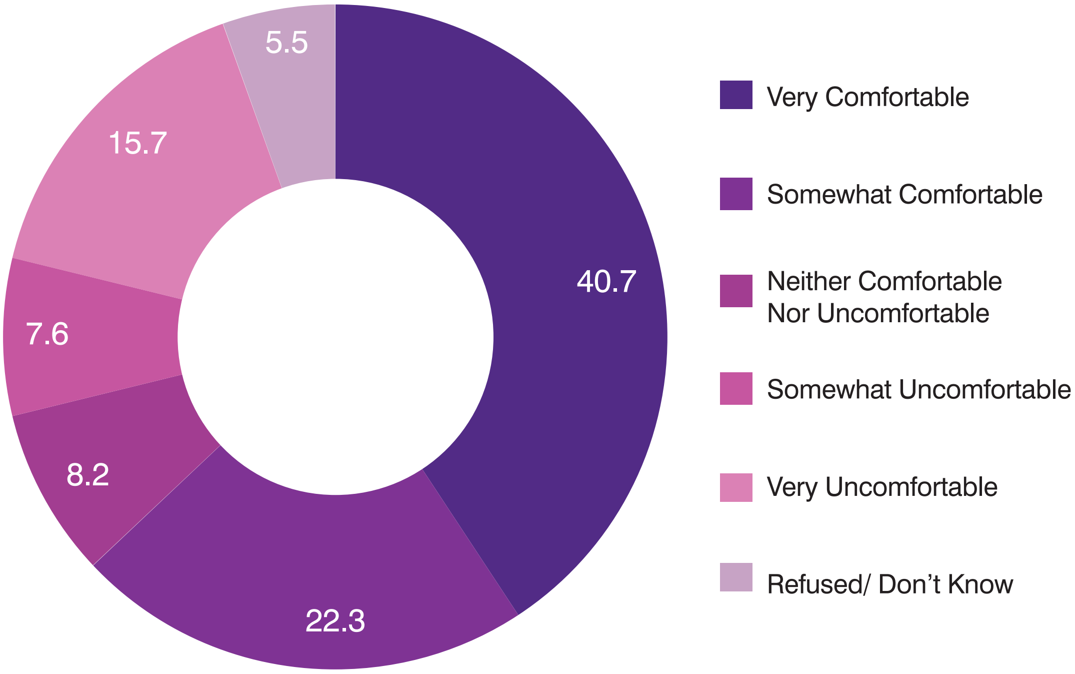
[70] Department of Home Security, *National Strategy for Information Sharing and Safeguarding,* 2012, https://www.dhs.gov/sites/default/files/publications/15_1026_NSI_National-Strategy-Information-Sharing-Safeguarding.pdf.

[71] Government of Canada, *Information Sharing for National Security,* https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/shrng-ns-nfrmtn-en.aspx.

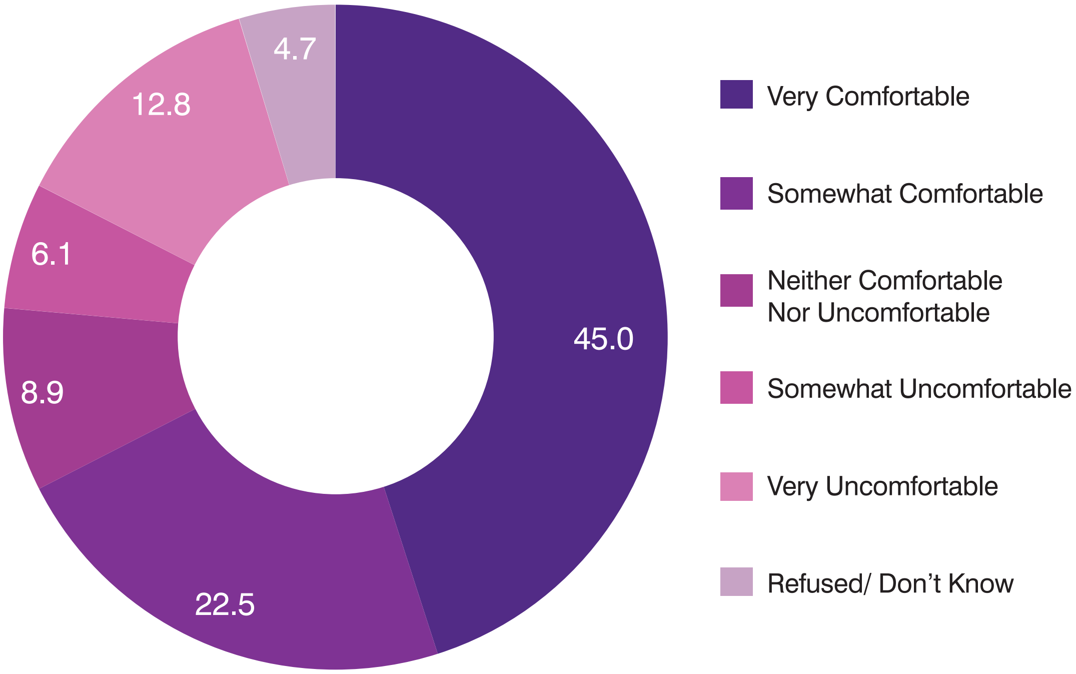
Would you be comfortable sharing your personal data, such as location data, to assist the government in its anti-terrorism efforts?



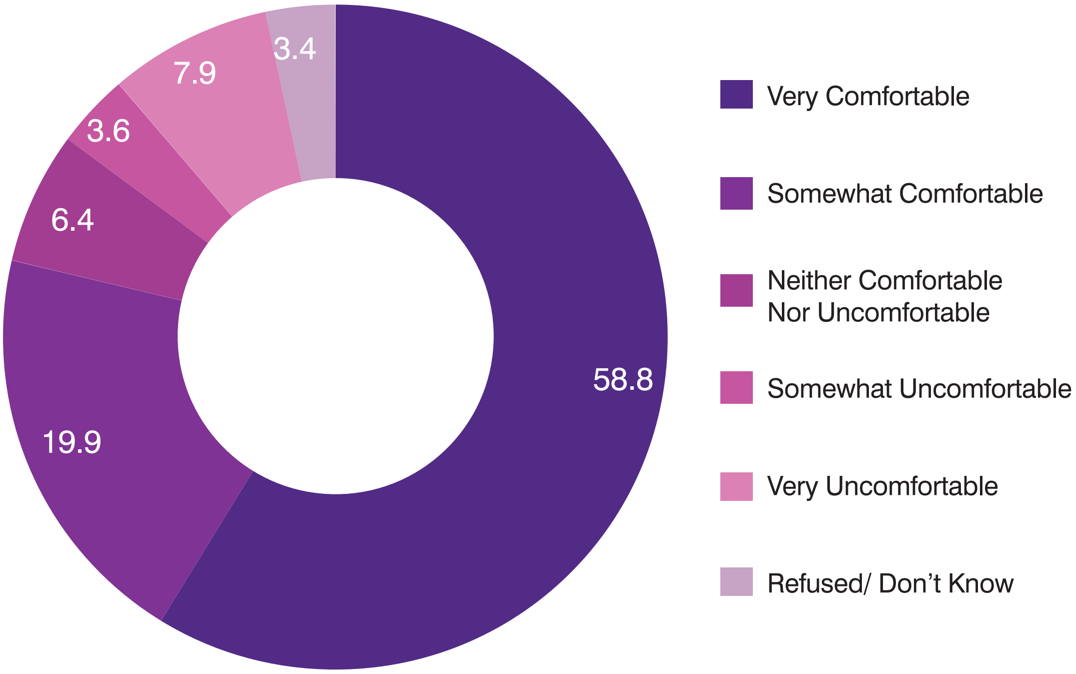
Would you be comfortable sharing your personal data, such as location data, to assist the government in stopping foreign interference in Indian elections?



Would you be comfortable sharing your personal data, such as financial data, to assist the government in reducing organised cyber crimes like financial fraud, hacking and ransomware attacks?

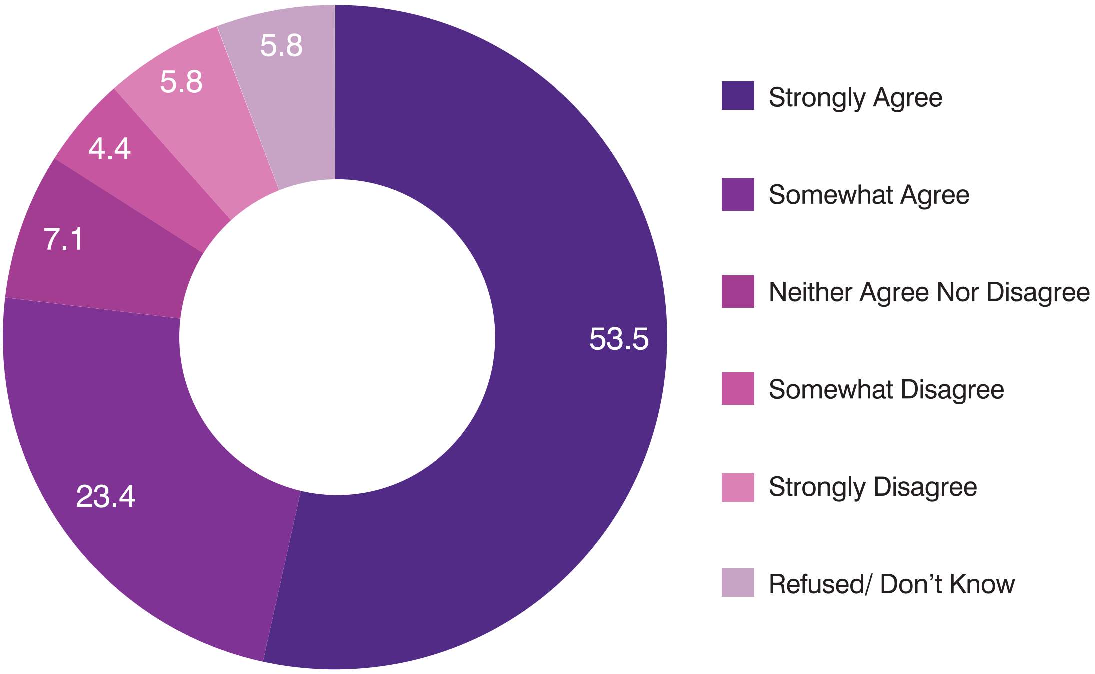


Would you be comfortable sharing your personal data, such as location data, to assist the government in ensuring road safety?



In February 2021, the Indian government made another proposal to prioritise national security and public concerns within the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[72] (IT Rules) under Section 87 of the IT Act. The sub-rule (2) of Rule 5 of the IT Rules requires social media intermediaries such as WhatsApp and Telegram, which offer end-to-end encryption (E2EE), to breach E2EE in order to identify the first originator of a particular message.[73] More than seven of every 10 respondents (77 percent) agree that for the government, concerns of public safety and national security are often more important than individual privacy. Nevertheless, concerns of privacy are not in contradiction to security; rather, they are part of the larger discussion on security as weakened encryption standards can be used by malicious actors to plan and execute cyberattacks.[74]

Are public safety and national security concerns often more important for the government over individual privacy?



[72] Ministry of Electronics and Information Technology, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021," https://mib.gov.in/sites/default/files/IT%28Intermediary%20 Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf.

[73] Internet Freedom Foundation, "Explainer: How the New IT Rules Take Away our Digital Rights" *The Wire*, February 26, 2021, https://thewire.in/tech/explainer-how-the-new-it-rules-take-away-our-digital-rights.

[74] Mieke Eoyang and Michael Garcia, *Weakened Encryption: The Threat to America's National Security,* *Third Way,* 2020, https://www.thirdway.org/report/weakened-encryption-the-threat-to-americas-national-security.

A conservative majority of the respondents (56.5 percent) expressed support for allowing foreign companies to share personal data with foreign law enforcement entities to reduce criminal activities on the Internet, while over a quarter (28 percent) opposed it. In August 2021, Apple Inc introduced certain proposals to reduce the proliferation of Child Sexual Abuse Material (CSAM) on the Internet.[75] One of the proposals that drew backlash from consumers[76] was allowing Apple to scan iCloud Photos, available locally on a consumer's phone or iPad, to find CSAM using NeuralHash that will break images into hashes. Every time an account shares such content and finds a match against the list of hashes by the National Centre for Missing and Exploited Children (NCEMC), it generates safety vouchers. If the number of vouchers exceeds the threshold,[77] the images get decrypted and are flagged for human moderators, who can disable the account and report it to the NCEMC.

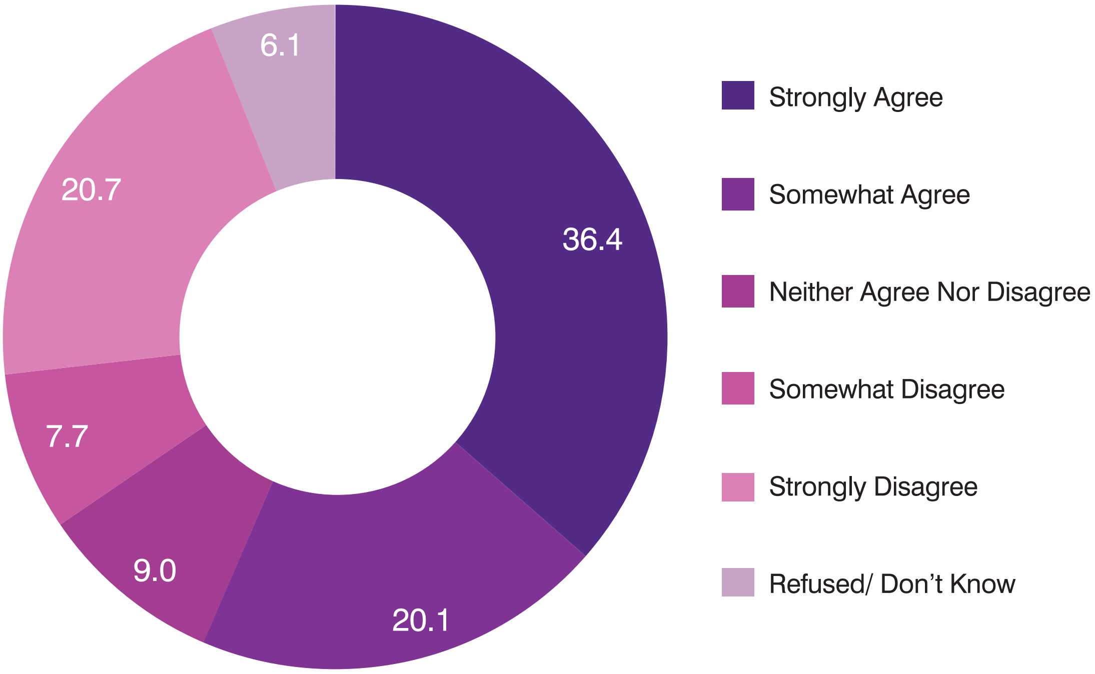
The strategy was supposed to be rolled out in the US first where, like in many other jurisdictions, it is illegal to possess CSAM. However, the plan has been delayed[78] as civil society organisations, academicians, and computer scientists opposed the proposal, arguing that these mechanisms undermine user privacy. About 55 percent of the respondents in this present survey expressed support for granting private companies access to photos on their phones to track the distribution of child sexual abuse material; 30 percent of the respondents opposed the idea.

[76] "An Open Letter Against Apple's Privacy-Invasive Content Scanning Technology" https://appleprivacyletter.com.

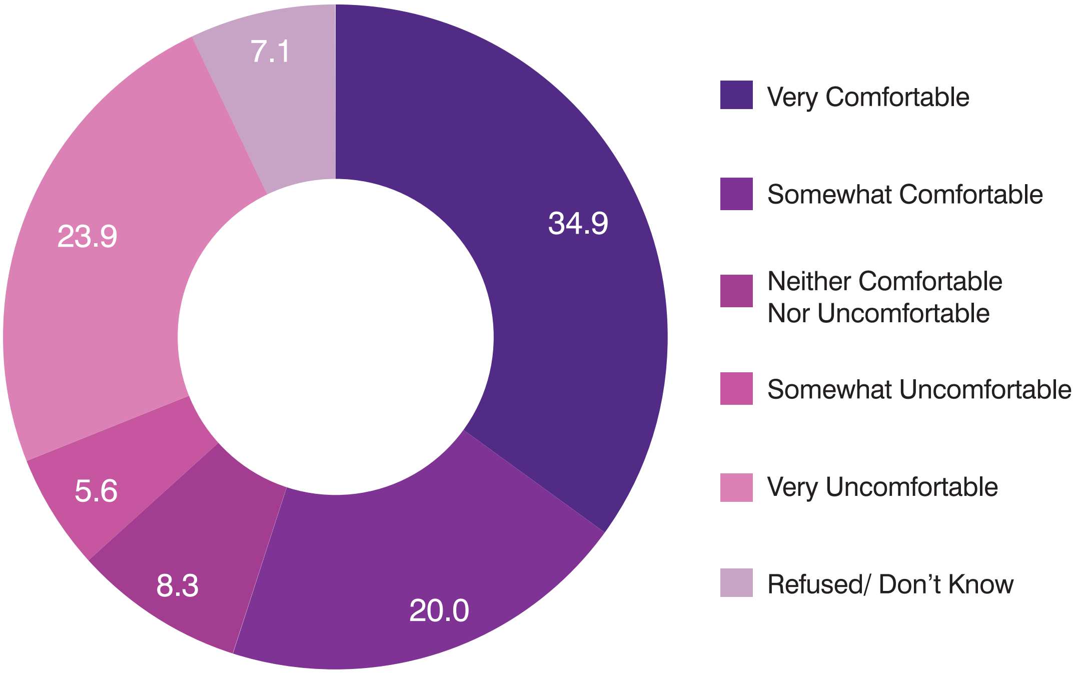
[77] Adi Robertson, "Apple's controversial new child protection features, explained," *The Verge*, August 10, 2021,https://www.theverge.com/2021/8/10/22613225/apple-csam-scanning-messages-child-safety-features-privacy-controversy-explained.

[78] David K. Li and Olivia Solon, "Apple delays plans to scan devices for child sexual abuse images," *NBC News,* September 4, 2021, https://www.nbcnews.com/tech/apple/apple-delays-plans-scan-devices-child-sexual-abuse-images-n1278459.

Do you support foreign companies being allowed to share personal data generated by Indians with foreign law enforcement agencies to prevent criminal activity on the Internet?



Would you be comfortable sharing access to the photos on your phone with private companies to track and minimise the distribution and creation of child sexual abuse material on the internet?



The survey found the highest proportion of respondents supporting data-sharing with third parties among the participants from East India (74.9-83.6 percent). When asked whether they are comfortable sharing access to photos on their phone with private companies to track and minimise the distribution and creation of CSAM, 75 percent of East Indians, 63.5 percent of South Indians, 48 percent of West Indians, and 47.5 percent of North Indians support the proposal. In the context of this question, the divergence between the proportions of responses from the youth of East and North India is highly statistically significant at the five-percent level.[79] The support for sharing data for concerns of national security is as low as 31 percent among respondents from North India, and 27 percent in West India.

East India—which had the highest proportion of respondents agreeing to data-sharing for national sovereignty and security—has been beset by internal and external security challenges. These include insurgencies[80] and transnational organised crimes such as human trafficking, and women[81] and child[82] sexual abuse.[83]

[79] Results of the test of significance for difference of proportions in large samples: Z score = 7.176, p-value is very close to zero

[80] Ministry of Home Affairs, *Insurgency in North East,* 2021, https://www.mha.gov.in/sites/default/files/InsurgencyNE_20092021.pdf.

[81] Based on the NCRB statistics on crimes against women, we compute the average of the crimes per lakh population across states for each zone of India namely, north, south, east and west. We find that the average crime rate per lakh population is the highest for east India at 55.25, followed by south, north and west India at 54.32, 54.15 and 35.56 respectively.

[82] Based on the NCRB statistics on crimes against children, the average crime rate per lakh population is the highest for east India at 31.55, followed by north, west and south India at 30.8, 30.6 and 28.7 respectively.

[83] Saratkumar Sharma, *Child Trafficking in the Indo-Myanmar Region: A Case-Study in Manipur,* Ministry of Women and Child Development, 2016, https://wcd.nic.in/sites/default/files/RESEARCH%20PROJECT%20REPORT_0.pdf.

A significant majority of both Gen-Z and millennial respondents support data-sharing with both Indian and foreign entities for national security purposes. Between 52–79 percent of the Gen-Z respondents and 57–78 percent of millennial respondents support data-sharing for the purposes of maintaining national sovereignty and security. Data-sharing for road safety received the highest support, with about 79 percent of both Gen-Z and millennials in agreement. On the question of whether for the government, concerns of national sovereignty and security supersede individual privacy, a significant majority of both Gen-Z (75.3 percent) and millennial respondents (77.8 percent) favoured the idea.

Support for data-sharing for national security cuts across gender in most cases of data sharing. However, while 54.8 percent of the female respondents are comfortable sharing access to photos on their phone with private companies to track and minimise the distribution and creation of CSAM, only 45.2 percent of the males are willing to do so. In this context, the deviation is statistically significant at the five-percent level of significance.[84] Among the Gen-Z respondents, 52.7 percent of the females said they would be comfortable sharing access to photos on their phone with private companies to bring CSAM under control; of the males, 52.5 percent are willing. Meanwhile, among the millennial respondents, the proportions are 56.3 percent for the females, and 57.1 percent for the males.

Broken down by region—71.4 percent of female respondents from the Eastern states are comfortable sharing access to their phones for anti-CSAM concerns, compared to 64.5 percent in South India, 50 percent in West India, and 47.2 percent in

[84] Results of the test of significance for difference of proportions in large samples: Z score = 4.292, p-value is very close to zero

North India. The difference in the responses of East and North Indian females is highly statistically significant at the five-percent level.[85] Similar disaggregation of responses about sharing access to locational data for road safety found that 92 percent of the female respondents from the Southern states are comfortable, then followed by females from East (89 percent), North (80 percent), and West (67 percent). The difference in the responses of South and West Indian females is highly statistically significant at the five-percent level.[86] Across all regions, there were more female respondents than males who support data-sharing for road safety.

The survey found that a majority of the employed respondents, and similarly a majority of those unemployed, agreed with the idea of data-sharing for reasons of national security, road safety, and others. A higher proportion of employed respondents (58-79 percent) than unemployed (52.9-79 percent) supported data-sharing for national security. The divergence is statistically significant at the five-percent level of significance. On the question of whether they are comfortable allowing foreign tech firms to share their personal data with foreign law enforcement agencies to prevent criminal activity on the internet, a conservative majority of both employed (58.5 percent) and unemployed (54.6 percent) respondents expressed their approval.

Respondents with higher levels of education, and those with lower levels, are in most instances at par in their support for data-sharing for national sovereignty and security. However, on the question of whether governments consider national security concerns as superseding interests emerging from individual privacy, there was more agreement from

[85] Results of the test of significance for difference of proportions in large samples: Z score = 6.3765, p-value is very close to zero

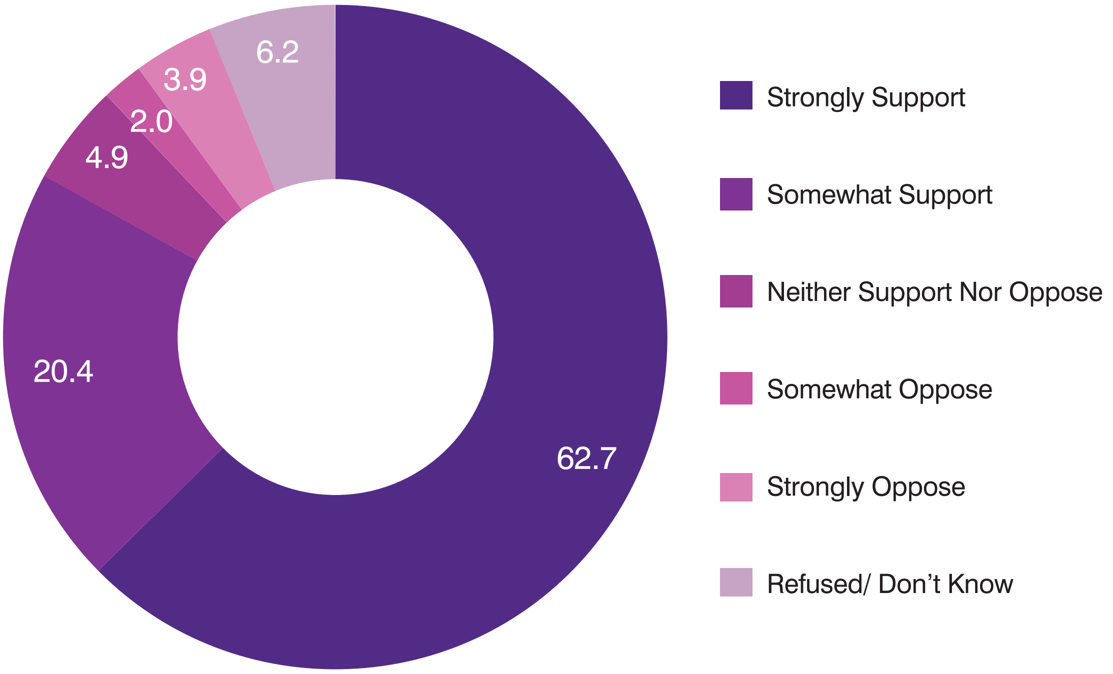
[86] Results of the test of significance for difference of proportions in large samples: Z score = 7.1136, p-value is very close to zero

respondents having higher levels of education (80 percent) than those with lower levels (74.3 percent). In the context of this question, the deviation between responses of the two sets of youth is significant at the five-percent level of significance.[87]

b) Technology protectionism

On the question of whether India should adopt regulations that will protect its domestic technology industry to be more competitive, 83 percent of respondents said they agree. Under the leadership of Prime Minister Narendra Modi, India has made a quick return to tech protectionism to address the country's large trade deficit and promote manufacturing capabilities.[88]

Should India adopt protectionist measures to ensure its domestic technology industry is internationally competitive?



[87] Results of the test of significance for difference of proportions in large samples: Z score = 2.9272, p-value = 0.0038

[88] Richard M. Rossow, Time for India's Tech Voices to Rise Against Digital Protectionism, Centre for Strategic and International Studies, 2021, https://www.csis.org/analysis/time-indias-tech-voices-rise-against-digital-protectionism.

A significant majority of respondents (more than 70 percent) from across all four regions support the implementation of protectionist policies for nurturing homegrown tech companies. Across employment status, a majority of both employed (84 percent) and unemployed (82.2 percent) respondents agree with the strategy. Broken down by gender, a majority of the males (82.8 percent) and females (83.24 percent) support the idea. Similarly, across age groups, both Gen-Z (82.3 percent) and millennial respondents (83.4 percent) support protectionism for the Indian technology sector.

There were more respondents with a higher level of education (87 percent) who support protectionist policies for the domestic tech industry, compared to those with a lower level of education (78.4 percent). The difference is statistically significant at the five-percent level of significance.[89] Disaggregating responses simultaneously by education and region, the findings show that irrespective of the level of education, at least 74 percent of the respondents across all regions support tech protectionism. However, there was a significant divergence in agreement between those with higher education and those who studied until Class XII or below, in both South and West India. About 87 percent of those with higher education in the Western and Southern states support tech protectionism, while 74 percent of respondents from these regions who studied till Class XII or below do so. The difference in responses of South and West India is statistically significant at the five-percent level.[90]

[89] Results of the test of significance for difference of proportions in large samples: Z score = 5.0443, p-value is very close to zero.

[90] Results of the test of significance for difference of proportions in large samples:
South India : Z score = 3.8086, p-value = 0.00014
West India : Z score = 3.7242, p-value = 0.0002

c) International collaboration

India is among the top five regions in the world facing the gravest threats of cyberattacks, in particular, cyber espionage with the intention of collecting business, geopolitical and military intelligence.[91] This comes amidst the ongoing review of the country's National Cybersecurity Policy (NCP).[92] (India still relies on its old NCP, released in 2013,[93] even as its offensive cyber capabilities have evolved at a rapid pace.) The authorities responsible for cyber security—the National Cyber Coordination Centre subordinate to CERT-In for civil, and the Defence Cyber Agency for the military—became functional only in 2018 and 2019, respectively.[94] Furthermore, India's offensive cyber capabilities are dispersed and only regionally effective. Eight of every 10 respondents (80 percent) support India investing in offensive cyber operations as part of its National Security Strategy. Respondents believe that this will protect India against nations engaging in electronic or physical warfare.

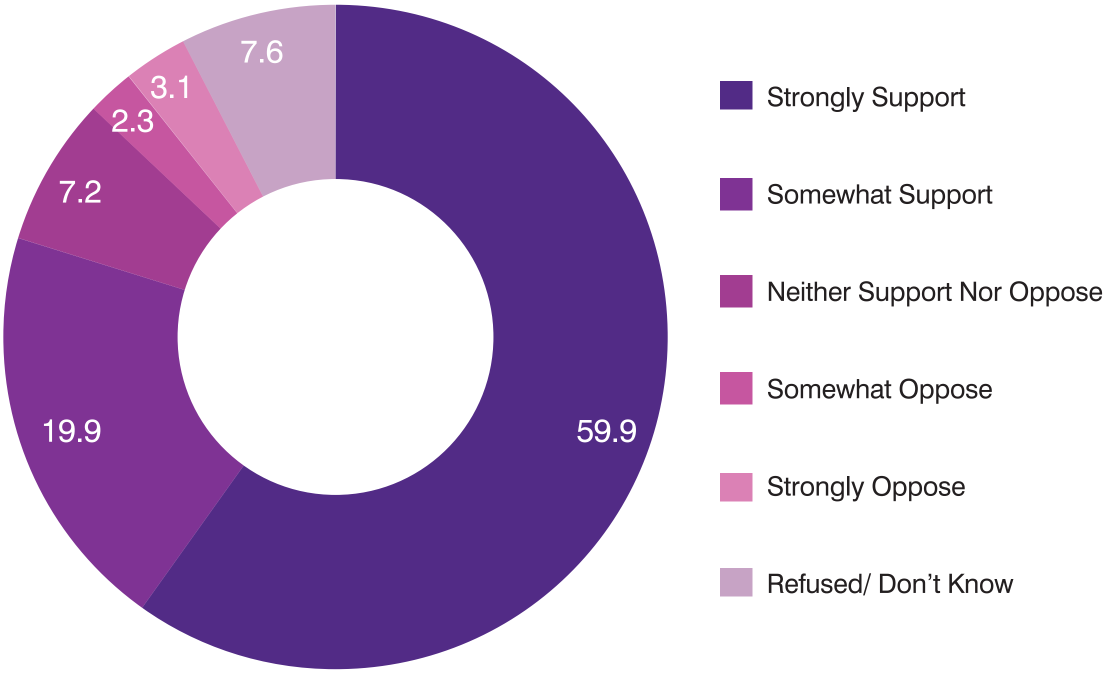
[91] "Kaspersky predicts rise in cyber espionage for India in 2022," *Business Standard,* January 14, 2022 , https://www.business-standard.com/article/economy-policy/kaspersky-predicts-rise-in-cyber-espionage-for-india-in-2022-122011401057_1.html.

[92] IANS. "India in final stages of clearing national cybersecurity strategy". *Business Standard.* October 27, 2021, https://www.business-standard.com/article/current-affairs/india-in-final-stages-of-clearing-national-cybersecurity-strategy-121102700663_1.html.

[93] Ministry of Communication and Information Technology, *National Cyber Security Policy,* 2013, https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf.

[94] International Institute for Strategic Studies, *Cyber Capabilities and National Power: A Net Assessment,* 2021, https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

As a national security strategy, should India invest in offensive cyber operations to protect the functionality of its infrastructure projects against nations engaging in electronic or physical warfare?



India is also engaging in several multilateral and bilateral partnerships such as the QUAD,[95] Comprehensive Strategic Partnership with Australia,[96] and the Global Partnership on AI.[97] These platforms are designed to enhance the partners' technological capabilities,[98] and effectively deal with cyber threats[99,100] and risks emanating from new technologies. Eighty percent of respondents support India's increased engagement and cooperation with international partners on

[95] ORF. *The QUAD - Alliance for a Prosperous Indo-Pacific,* https://www.orfonline.org/series/the-quad-age-alliance-for-a-prosperous-indo-pacific/.

[96] Department of Foreign Affairs and Trade, *Joint Statement on a Comprehensive Strategic Partnership between Republic of India and Australia,* 2020 https://www.dfat.gov.au/geo/india/joint-statement-comprehensive-strategic-partnership-between-republic-india-and-australia.

[97] "Global Partnership on AI" https://gpai.ai.

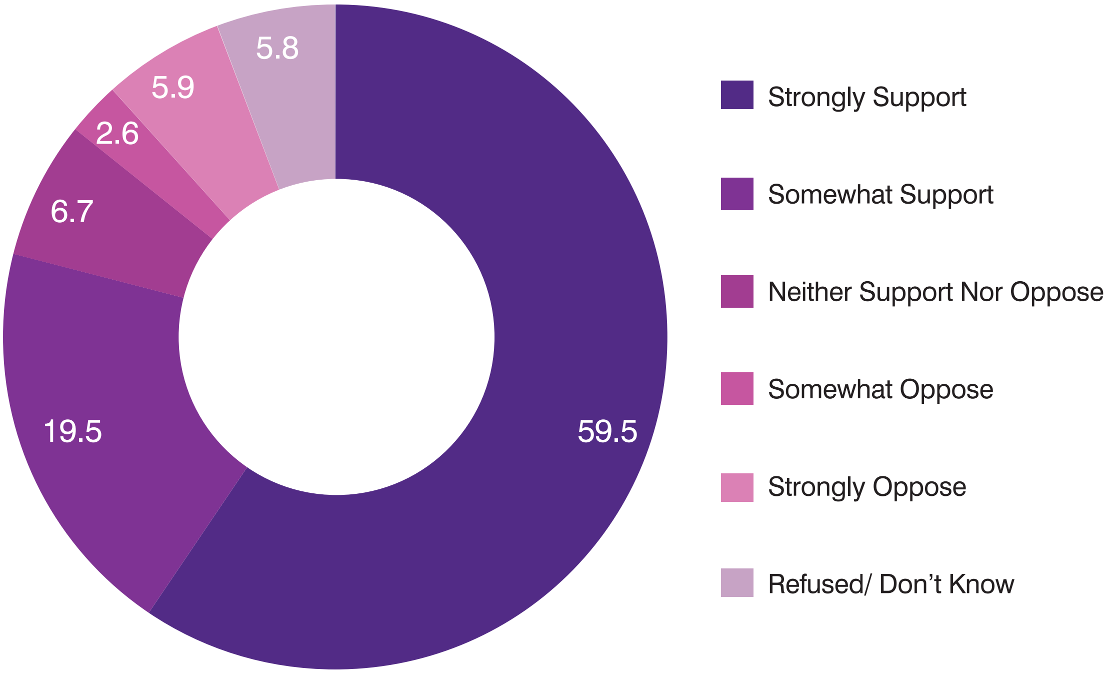
[98] Department of Science and Technology, *International S&T Cooperation,* https://dst.gov.in/international-st-cooperation.

[98] Ministry of Electronics and Information Technology, International R&D Collaboration, https://www.meity.gov.in/international-rd-collaboration.

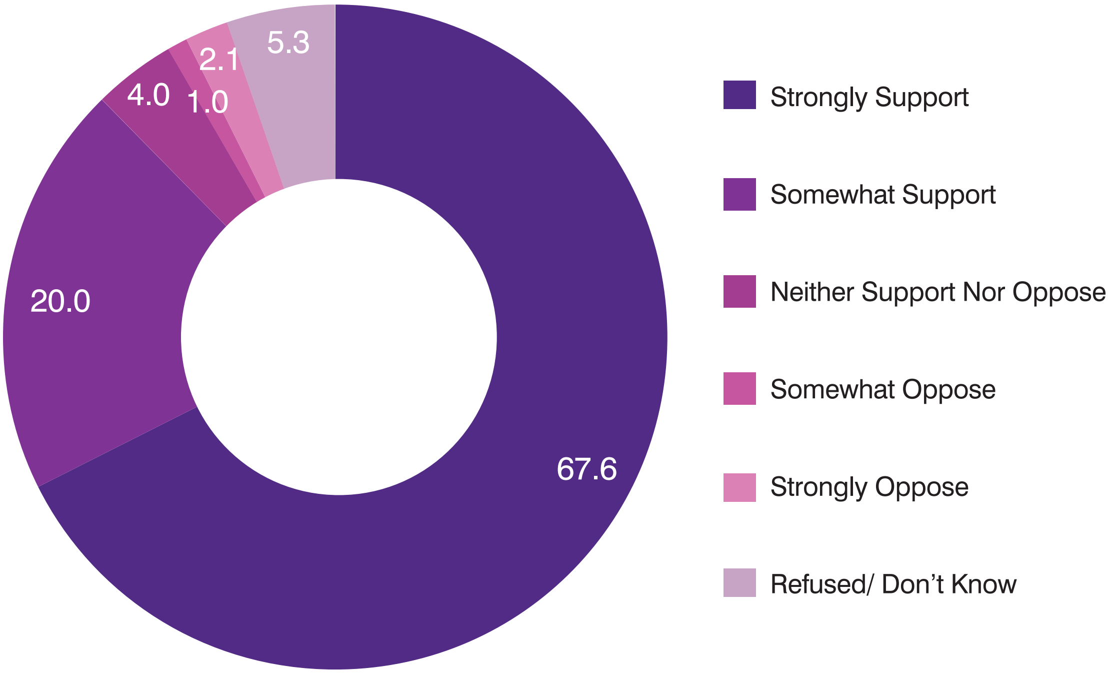
[100] India Science and Technology Innovation, *International collaborations boosting expertise,* leveraging S&T, https://www.indiascienceandtechnology.gov.in/listingpage/international-collaborations-boosting-expertise-leveraging-st.

technology-related concerns such as the risks to privacy and security posed by AI. Seventy-nine percent of respondents support building international coalitions that will impose economic sanctions on nations that use technology to identify citizens' voting preferences and interfere with domestic elections. More than six of every 10 respondents (68 percent) are in favour of holding accountable to international law those countries that house non-state actors responsible for hacking campaigns against critical public infrastructures such as healthcare, electricity, and telecommunications.

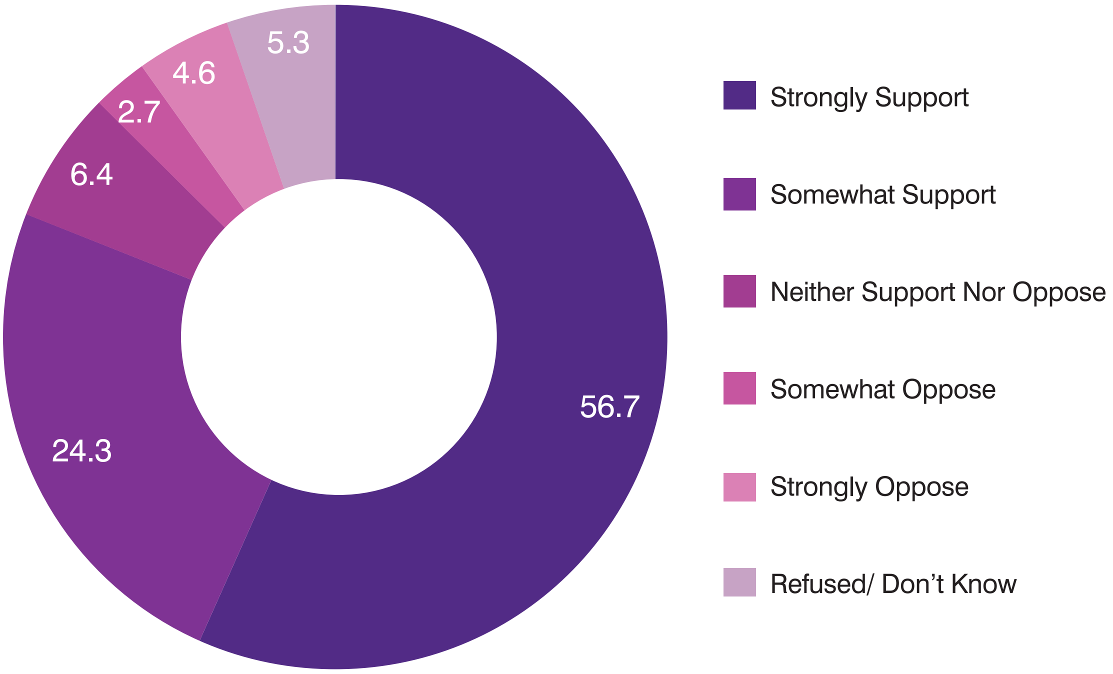
Should India support international coalitions that propose imposing economic sanctions on countries using technology to interfere in foreign elections, for instance, by identifying citizen's voting preferences?



Should the Indian government support imposing punishments, under international law, on countries housing cyber criminal groups as a deterrence to the rise in cybercrimes?



Do you support countries cooperating with each other to minimise privacy and security risks that are arising out of newer technologies like AI?



A significant majority of respondents from across the four regions (>70 percent) support the country's participation in multilateral initiatives that target cyber criminality. Similarly, a majority of both the males (79.4-87.5 percent) and females (77.7-87.7 percent) support the proposition.

Both Gen-Z and millennial respondents largely support India's participation in international collaborative measures that enhance cybersecurity. About 78-85 percent of the Gen-Z respondents, and 80-89 percent of the millennial respondents, support international collaboration and multilateralism in ensuring national security. Both Gen-Z (85.5 percent) and millennial respondents (89 percent) agree with the proposition of the Indian government endorsing the punishment, under international law, of countries housing cyber-criminal groups.

A higher percentage of the employed respondents (80-89 percent) support India's participation in multilateral initiatives targeting cyber criminality, as compared to those unemployed (76-86 percent). The most remarkable divergence between the responses of the employed and the unemployed youth is observed in the context of their support to India's investment in offensive cyber operations to protect its infrastructure projects against electronic or physical warfare. While 83.5 percent of the employed respondents support the proposition, 76.3 percent of the unemployed respondents do so. In the context of this proposition, the divergence is statistically significant at the five-percent level of significance.[101]

Disaggregating responses about India's investment in offensive cyber operations simultaneously by region and employment status, the difference in the responses between the employed respondents (86.7) and unemployed respondents (64.6

[101] Results of the test of significance for difference of proportions in large samples: Z score = 4.0076, p-value is very close to zero

percent) within South India was more pronounced than the other regions, and is statistically significant at the five-percent level.[102] Notably, 88.3 percent of unemployed respondents from West India support multilateral partnerships to deal with the risks posed by AI to privacy and security, as compared to 82.5 percent of employed respondents in the region. This difference is statistically insignificant at the five-percent level.[103]

There is greater support (83–90 percent) from among the respondents with higher levels of education for India's participation in multilateral initiatives targeting cyber criminality, compared to those with lower levels of education (74–84 percent). The divergence is statistically significant at the five-percent level of significance.

C. Economic Well-Being

a) The demand for a renewed vision of data-sharing

The current data-sharing system favours enterprises with proprietary algorithms that are able to exercise 'ownership' over the data of individuals and generate economic value from it.[104] India, with MeitY's expert committee on NPDGF, had attempted to regulate aggregated non-personal data and to make the social and economic value generated from data accessible to citizens and the society at large. As perfect anonymisation is still relatively difficult to achieve, non-personal data has been subsumed under the Data Protection Bill, 2021 and will also be regulated by the Data Protection Authority.

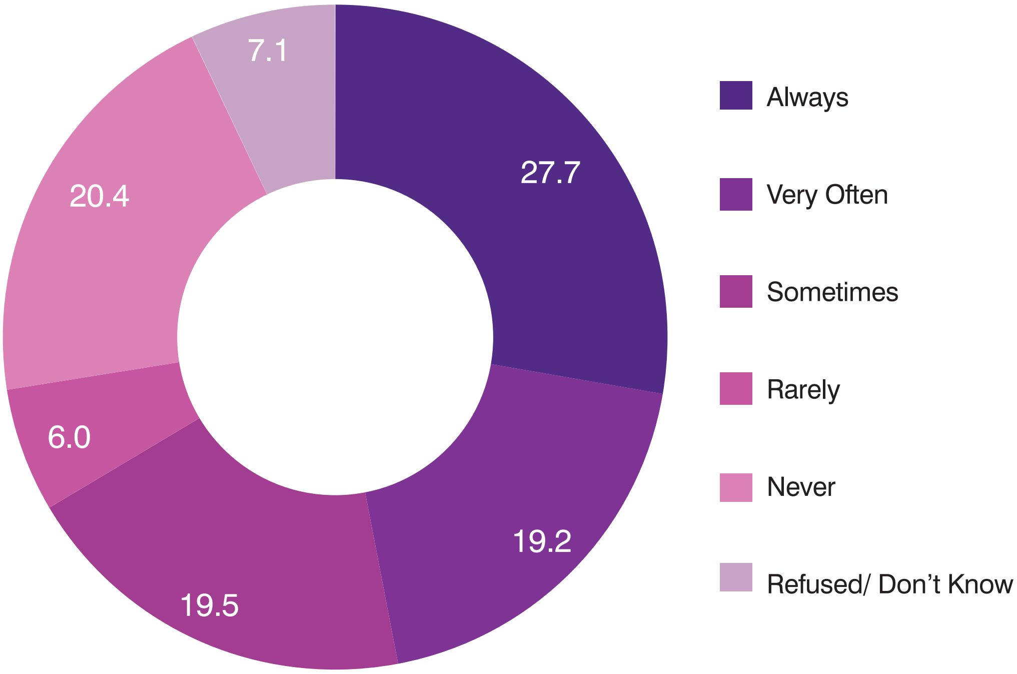
[102] Results of the test of significance for difference of proportions in large samples: Z score = 3.5487, p-value = 0.00038

[103] Results of the test of significance for difference of proportions in large samples: Z score = 1.8507, p-value = 0.06432

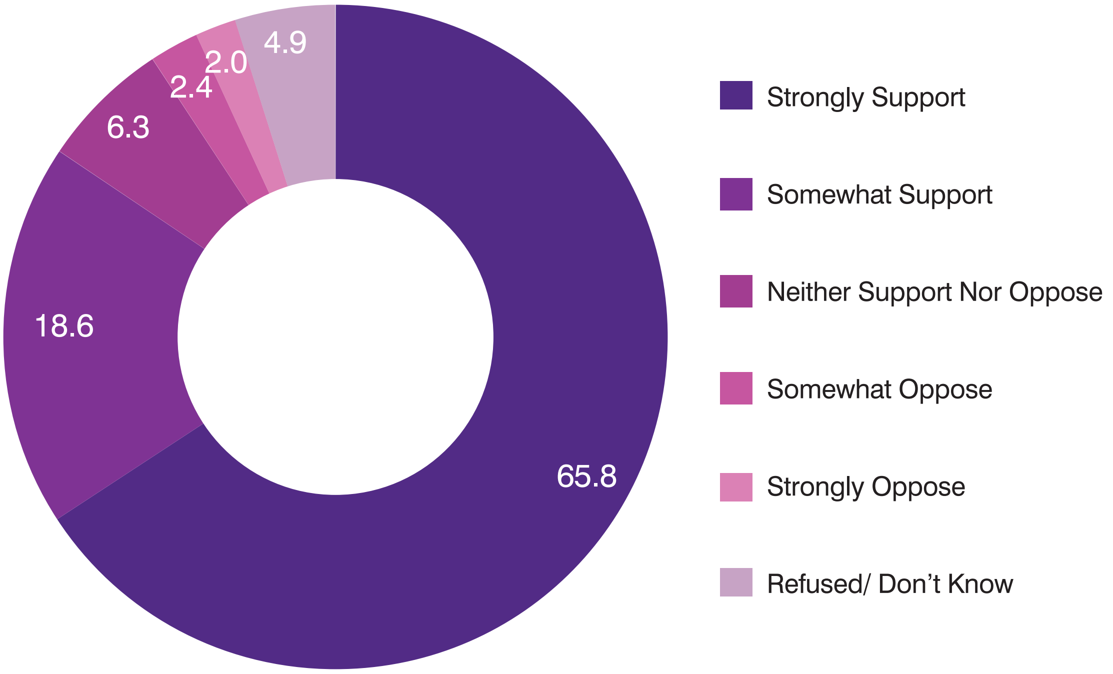
[104] Cameron F. Kerry and John B. Morris, Jr, *Why data ownership is the wrong approach to protecting privacy,* Brookings, 2019. https://www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/.

About 47 percent of the respondents believe that social media companies share their personal data with e-commerce platforms, and vice versa, to advertise products that bring benefits to consumers. A little over a quarter (26.4 percent) are of the opinion that such data-sharing is not for the benefit of consumers. Some 84.4 percent of respondents support the principle that government should impose higher fines for foreign companies that violate privacy laws, as compared to domestic companies that commit similar transgressions. A significant majority (84–90.2 percent) of respondents from all four regions of the country support this proposition.

How often do you think e-commerce websites share your personal information including information on last searched item with social media platforms to show you relevant product advertisements?



Should foreign companies violating privacy laws laid down by the Indian government be given harsher punishments e.g., more fines than Indian companies committing similar violations?

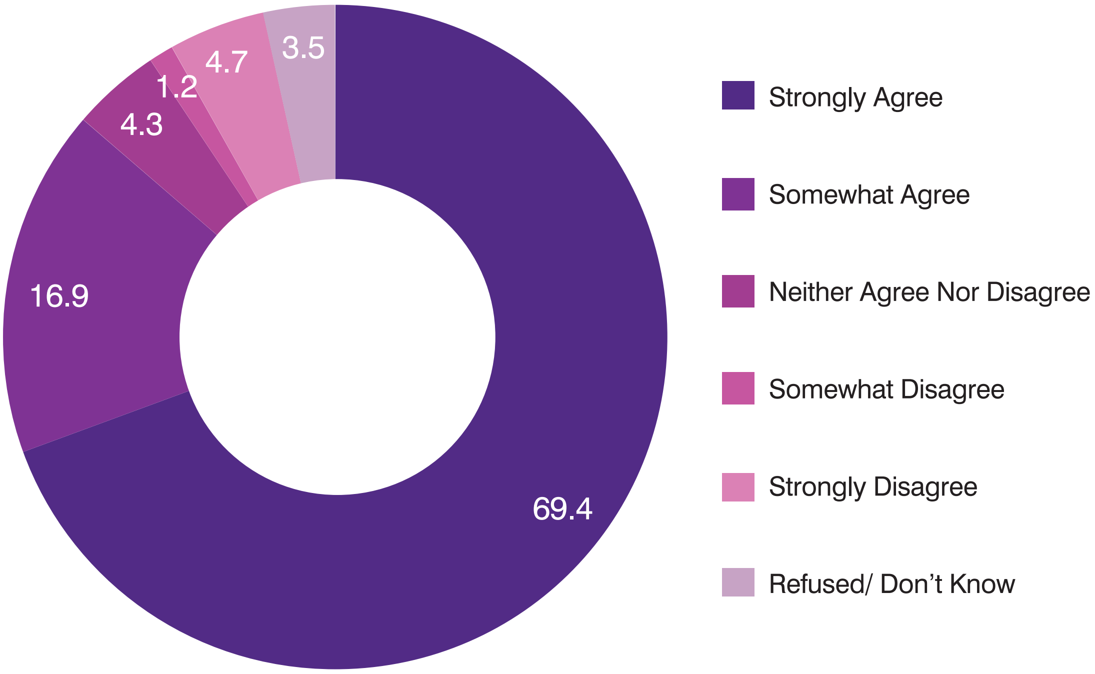


As part of the IT Rules 2021, social media intermediaries, under due diligence requirements, must inform users within their 'user agreement' that they are not permitted to upload, publish or share information that is "patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person, entity or agency for financial gain or to cause any injury to any person."[105] Moreover, the platforms have the right to terminate access or usage rights to the account and remove information that does not comply with the standards outlined within their community guidelines and is unlawful information relating to the sovereignty and integrity of India, or decency or morality. This is to be done after receiving a notification from the government or appropriate agency, as stated in clause

[105] MeiTy, IT Rules, *2021*

(b) of sub-section (3) of Section 79 of the IT Act. A large majority of the respondents (86.4 percent) also agree that the government should impose fines on these intermediaries if their platform is misused to spread rumours that could potentially challenge the credibility of users or pose a threat to their jobs. A majority of respondents (83—92 percent) from all regions support this idea.

Should social media platforms be fined or penalised if their platforms get misused to spread rumours which can potentially challenge your credibility and pose a threat to your job?



Section 79 of the IT Act provides protection to social media intermediaries from being held liable for content and communication made by the users on the platform as long as they are compliant with the established due diligence requirements. Increasingly, however, governments are rethinking the current blanket exemptions provided to digital platforms. For instance, the 2017 Network Enforcement

[106] The Bundestag, Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken, 2017, https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html.

Act[106] in Germany, aimed at combating fake news and hate speech on online platforms, mandates platforms to remove “clearly illegal content” in a stipulated time period or else face huge fines. In India, in addition to the government, the Supreme Court has also called on platforms to actively monitor content and ensure compliance with existing laws designed to protect women and children.[107] Indeed, a 2018 study by Amnesty International found that Twitter’s inability to deal with violent content on its platform is compelling women, including politicians and journalists, to limit their use of the platform.[108] At the same time, however, stringent action by the government on criteria that are as yet vague could also potentially lead to platforms censoring content and violating users’ freedom of expression.

On the question of extracting economic benefits from voluntary data sharing, 66 percent of the respondents stated they are not comfortable with selling their data in exchange for monetary compensation from Big Tech companies. An example of this is Amazon, which in August 2021 offered consumers INR 700 (~US$10) for their palm print if they would enrol in its palm print recognition system, Amazon One.[109] The system assists consumers in paying for the products at physical Amazon markets with the help of palm scans. Unlike an interest or a hobby tracked by algorithm, which does not necessarily trace back to a unique individual, biometric information is unchangeable and acts as a unique identifier; its exchange can significantly increase security risks for the individual. While a majority (66.3 percent) are not in favour of selling biometric data, around 21 percent of respondents are

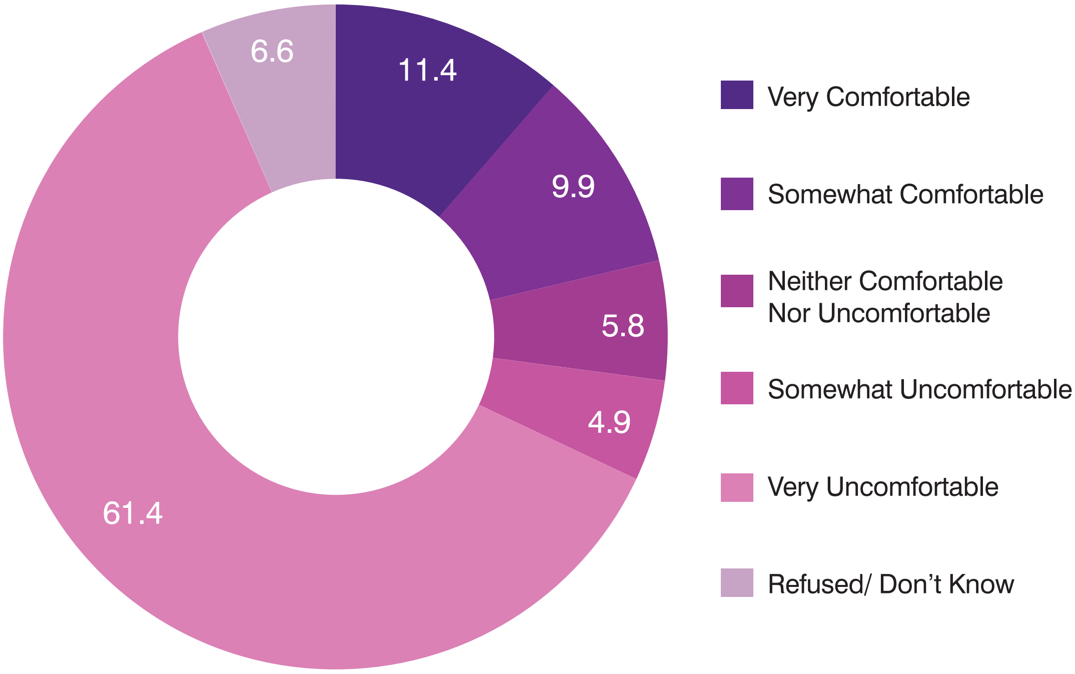
[107] Vikram Jeet Singh and Prashant Mara, “India: Intermediary Liability In India - Moving Goalposts” *Mondaq*, July 8, 2021, https://www.mondaq.com/india/social-media/1088968/intermediary-liability-in-india--moving-goalposts.

[108] Amnesty International, Toxic Twitter - *A Toxic Place for Women,* 2018, https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/.

[109] James Vincent, “Amazon will give you a whole $10 for your palm print,” *The Verge*, August 3, 2021, https://www.google.com/url?q=https://www.theverge.com/2021/8/3/22607218/amazon-one-palm-print-technology-10-dollar-promo&sa=D&source=docs&ust=1644677128354539&usg=AOvVaw2f5rAwLL-1SmS0eyiL-eYn.

comfortable with the idea. Across the four regions, respondents who are willing to sell their biometric data are far less than a majority. In North India, 75.1 percent of the respondents oppose the idea of selling their biometric data, while 68 percent of respondents from the West, 66.5 percent of respondents from the East, and 52.1 percent of respondents from the South do so.

Would you be comfortable selling your biometric data like eye or fingerprint scan in exchange for some amount, say INR700?



Broken down by age group, both Gen-Z and millennial respondents demand the regulation of sharing data and do not approve of data-sharing for economic gains. A significant majority of both groups (82-85 percent for Gen-Z, and 86-87 percent for millennials) support the principle of imposing harsher punishments on foreign firms for violating Indian laws, as well as heavy penalties on social media companies if they allow their platforms to be misused to spread rumours and defame others. A small percentage of respondents of Gen-Z (19.3 percent) and millennials (22.8 percent) support the selling of one’s biometric data for economic gains.

A higher proportion of male respondents (88 percent) than females (84.5 percent) agree that penalties should be imposed on social media companies following their misuse for defamation. In the context of this question, the gender divergence is statistically significant at the five-percent level.[110] On disaggregating responses simultaneously by gender and employment status, there is no significant gender deviation in both the employed and unemployed. In most cases that involve demanding the regulation of such sharing and denying data for economic gains, there are equal proportions of male and female respondents who support the proposition.

A greater proportion of respondents with a higher level of education agree that data-sharing should be regulated and that data should not be shared for economic gains. Of the respondents with a higher level of education, 90 percent support imposing a penalty on the misuse of social media platforms; the proportion is 82.4 percent for those with a lower level of education. In the context of this question, the divergence is statistically significant at the five-percent level.[111] Meanwhile, 52.9 percent of respondents with a higher level of education believe that e-commerce websites share users' personal information to advertise products of their choice, while 40.2 percent of respondents with a lower level of education do so. This divergence is statistically significant at the five-percent level.[112]

[110] Results of the test of significance for difference of proportions in large samples: Z score = 2.2768, p-value = 0.0226

[111] Results of the test of significance for difference of proportions in large samples: Z score = 4.8124, p-value is very close to zero

[112] Results of the test of significance for difference of proportions in large samples: Z score = 5.677, p-value is very close to zero

Across employment status, a majority of both employed (87.3-88.5 percent) and unemployed respondents (81.7-84.4 percent) support harsher punishments for foreign firms that violate Indian privacy laws, as well as penalties on social media platforms that allow their misuse. The divergences are statistically significant at the five-percent level. A small percentage of unemployed (22.4 percent) and employed respondents (20.3 percent) support the selling of one's biometric data for personal financial gain. On disaggregating responses simultaneously by gender and employment status, male respondents are more willing to sell their biometric data than their female counterparts, irrespective of employment status. This deviation is statistically insignificant in the case of unemployed female (22 percent) and male respondents (23 percent),[113] but statistically significant for employed female (15 percent) and male (22 percent) respondents,[114] at the five-percent level of significance.

b) Data sharing for the public good

In 2012, former Karnataka high court judge Justice K.S. Puttaswamy challenged the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services Act, 2016[115] in the Supreme Court on two key premises: (1) inadequate safeguards against the misuse of data by the public or private sector; and (2) the principle that social security measures should not be contingent upon the ability to produce an Aadhaar card. The Aadhaar initiative, while intended to provide a singular identity for Indian residents, is

[113] Results of the test of significance for difference of proportions in large samples: Z score = 0.3606, p-value = 0.71884

[114] Results of the test of significance for difference of proportions in large samples: Z score = 2.3966, p-value = 0.0164

[115] Ministry of Law and Justice, Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.

increasingly being used as a basis for identifying beneficiaries of numerous welfare schemes including the Mid-Day Meal, Public Distribution System, and the Mahatma Gandhi National Rural Employment Guarantee Scheme.[116] The Supreme Court judgement in September 2018 upheld the Aadhaar Act, 2016 and noted that privacy is not an absolute right and that the law empowers the disenfranchised.[117,118] Infosys co-founder Kris Gopalakrishnan also said, "Data should be treated as a strategic asset at a national level. It is important for policy making, improving public service, and supporting a wide range of societal objectives including science, healthcare and so on."[119]

In this present survey, 82 percent of respondents support sharing their personal information like financial records to assist the government in providing rations or cash to the country's poor populations. Some 77.4 percent of respondents also support sharing medical records for maintaining a robust healthcare record system.

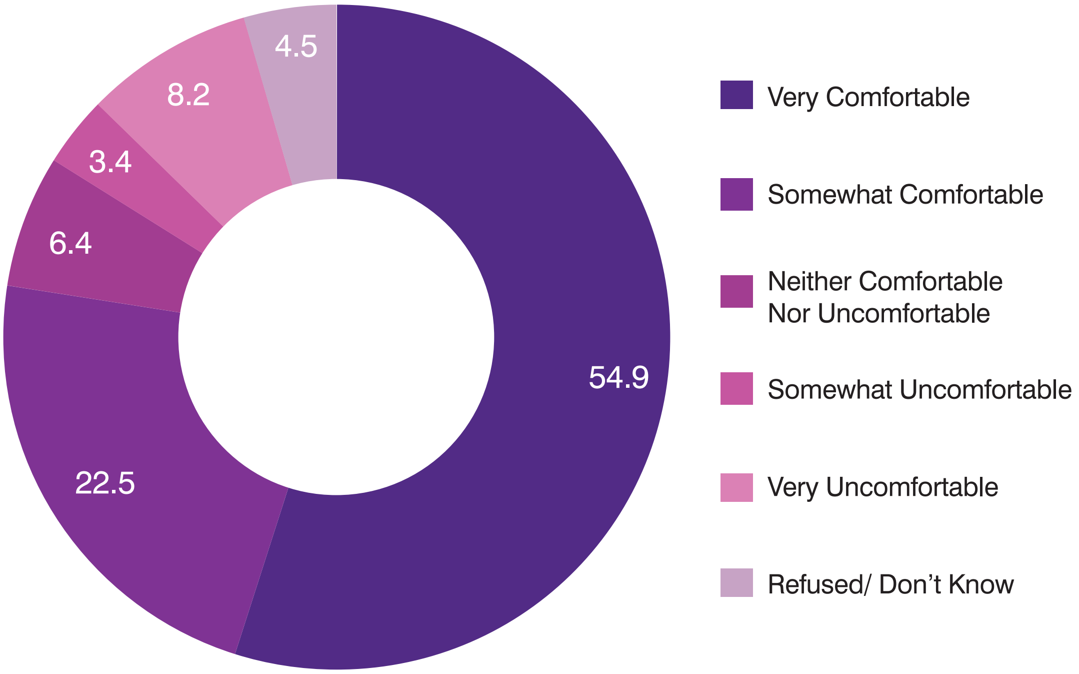
[116] PTI, "Govt. gets mandate to seek Aadhaar from beneficiaries under Social Security Code," *Mint*, May 5, 2021, https://www.livemint.com/news/india/govt-gets-mandate-to-seek-aadhaar-from-beneficiaries-under-social-security-code-11620214996570.html.

[117] Supreme Court Observer, *Constitutionality of Aadhaar Act,* 2018, https://www.scobserver.in/cases/puttaswamy-v-union-of-india-constitutionality-of-aadhaar-act-case-background/.

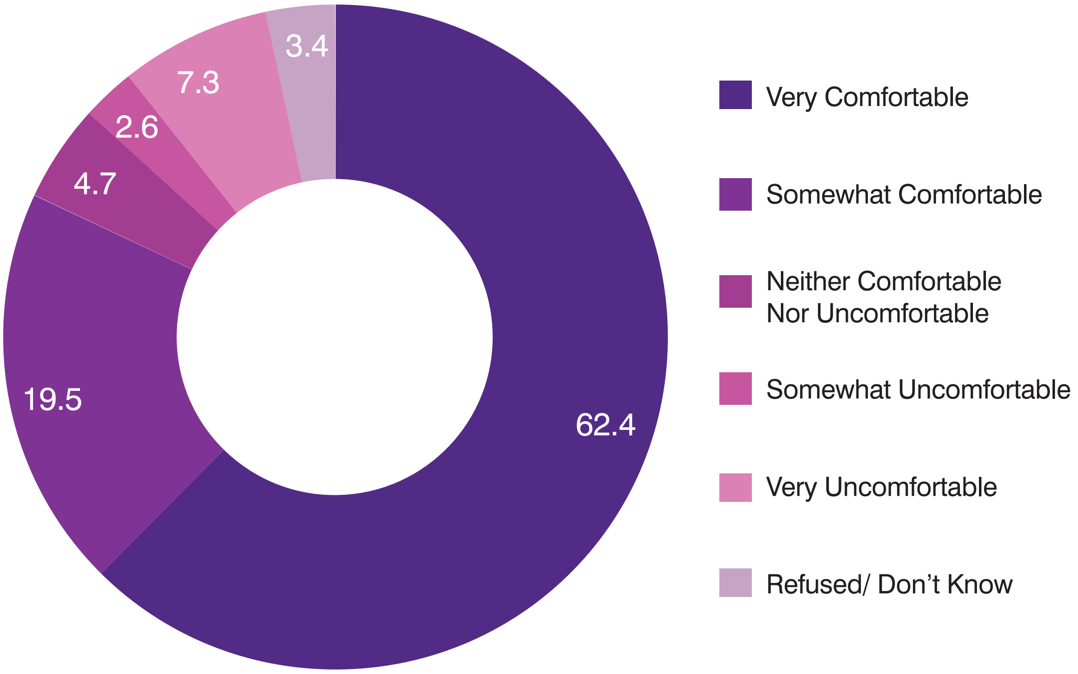
[118] Lalit Chandak, *Privacy and National Security - a National Need,* TRAI, 2017, https://trai.gov.in/sites/default/files/Span_Technology_07_11_2017.pdf.

[119] Office of the Principal Scientific Adviser to the Government of India and IIT Madras Alumni Association. *Science and Technology in the New Normal in India - A Public Attitude Study,* 2021, https://www.indiascienceandtechnology.gov.in/stihighlights/sti-era-new-normal-—-survey-report.

Would you be comfortable sharing your personal data like medical records to assist the government in avoiding public health emergencies by maintaining a robust healthcare record for national health insurances?



Would you be comfortable sharing your personal data, such as financial records, to assist the government in providing ration or cash to the poor?



East India has the highest proportion of respondents (91.1 percent) who support the sharing of data for public good, such as maintaining a robust healthcare record for national health insurances. In comparison, 86.3 percent of respondents in South India, 75.7 percent in North India, and 64.8 percent in West India support such a move. The difference between those who extend the highest support (East) and the lowest (West) to this proposition is highly statistically significant at the five-percent level.[120] More than nine of every 10 respondents (90.2 percent) from both East and South India are comfortable with sharing their data to assist the government in providing rations to the poor.

A majority of both Gen-Z (77–83 percent) and millennial respondents (78–81 percent) support sharing data for the public good. The same trend emerges in the context of gender, and employment. Therefore, irrespective of age, gender, and status of employment, a majority of respondents are comfortable with sharing data for the public good. Notably, on disaggregating responses in this context simultaneously by region and age, there is no significant age-related deviations among respondents from the South, East and North India. South India leads in this regard, with about 90 percent of both millennial and Gen-Z respondents supporting the sharing of financial data to provide rations to the poor. As far as West India is concerned, 66.2 percent of millennial and 72.1 percent of Gen-Z respondents support the proposition. However, this age-related difference is statistically insignificant at the five-percent level.[121]

[120] Results of the test of significance for difference of proportions in large samples: Z score = 7.4016, p-value is very close to zero

[121] Results of the test of significance for difference of proportions in large samples: Z score = 1.376, p-value = 0.16758

A majority of respondents among those with a higher (79.4–82.5 percent) as well as lower level of education (75.2–81.1 percent) support sharing data for the public good. There is a higher proportion of respondents among the highly educated (79.4 percent) than among those with lower levels of education (75.2 percent) who support data-sharing for maintaining a robust healthcare record for national health insurances and avoiding public health emergencies. In the context of this question, the divergence is statistically significant at the five-percent level.[122]

c) Data sharing to empower data principals

In August 2020, NITI Aayog released the draft DEPA document for comments from public stakeholders. It proposed a data-sharing framework that built on the Electronic Consent Framework V1.1 and Account Aggregator Framework. The implementation of DEPA is being tested across sectors, including healthcare[123] and financial services.[124] This framework seeks to give citizens (or data principals)[125] control over their data throughout the life cycle of data-sharing. In the context of financial services, this framework is intended to accelerate financial inclusion.

[122] Results of the test of significance for difference of proportions in large samples: Z score = 2.2424, p-value = 0.0251

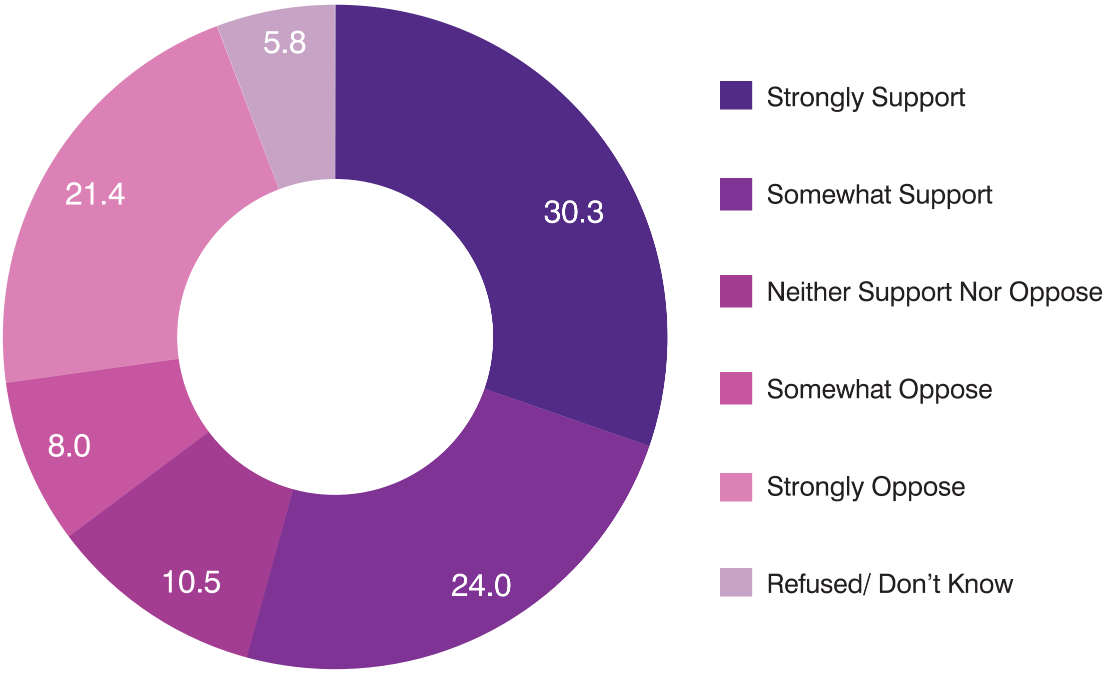
[123] Chandrashekar Srinivasan,"Health ID For Each Indian": PM Announces National Digital Health Mission," NDTV, August 15, 2020, https://www.ndtv.com/india-news/national-digital-health-mission-pm-modi-independence-day-speech-national-digital-health-mission-to-revolutionise-health-sector-says-pm-modi-2279792.

[124] Livemint, "Account Aggregators: These banks have joined it, how it will benefit consumers". *Mint*, September 12, 2021, https://www.livemint.com/money/personal-finance/account-aggregators-these-banks-have-joined-it-how-it-will-benefit-customers-11631417562966.html.

[125] Data Principal is the natural person to whom the personal data relates to. Deloitte "India Draft Personal Data Protection Bill, 2018 and EU General Data Protection Regulation: A comparative view.". (2019) https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-india-draft-personal-data-protection-bill-noexp.pdf.

DEPA is a public-private partnership to streamline the process of data-sharing for citizens and introduces stakeholders like third-party consent managers[126] in the data-sharing life cycle. More than five of every 10 respondents (54.3 percent) support the introduction of independent organisations to assist the simplification of data-sharing and re-provision of personal information—for example, details of previous loans to banks in case of application for new loans. Over a quarter of respondents (29.4 percent) do not support the proposition. Sixty-seven percent of respondents from South India, 62.4 percent of those from East India, and 51 percent of those from West India support the introduction of data intermediaries. Among respondents from the North, a lower 44.3 percent are in agreement.

Do you think independent establishments could assist in simplifying the process of sharing your personal details and physical documents like signatures, property papers, and details of previous loans to banks when applying for new loans to make the process of data sharing easier?



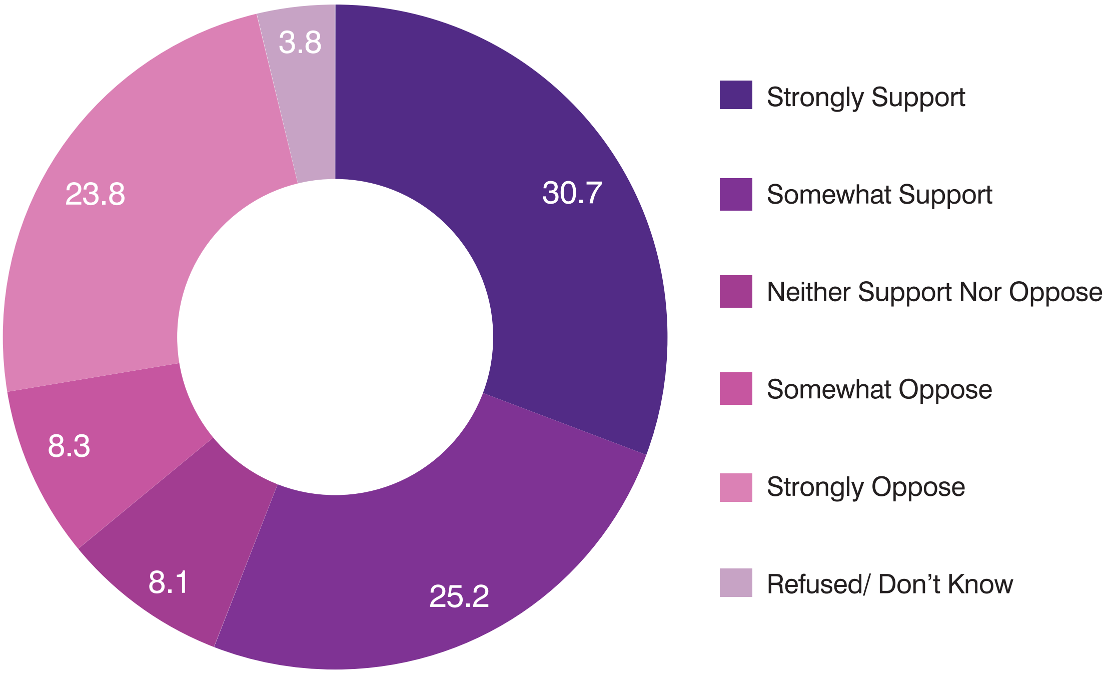
[126] Vikas Kathuria, *Data Empowerment and Protection Architecture: Concept and Assessment,* ORF Issue Brief No. 487, August 2021, Observer Research Foundation. https://www.orfonline.org/research/data-empowerment-and-protection-architecture-concept-and-assessment/#_edn2.

There is a statistically significant higher proportion of employed respondents who support the proposition—56.8 percent of employed respondents as compared to 51.9 percent of the unemployed—that independent entities assist in simplifying the process of sharing personal data and physical documents with banks in cases of new loan applications.[127] On disaggregating responses in this context simultaneously by region and employment status, the employment-related difference in the intensity of support is similar across all four regions.

Moreover, 56 percent of the respondents were in support of data controllers such as banks and hospitals sharing the medical and financial history of data principals to make interoperability easier when citizens move to another service provider. In the health sector, the Health Data Management policy is also based on digitising healthcare records to build an interoperable network for easy access to healthcare facilities while ensuring compliance with consent framework and personal data protection. There are significant regional deviations in the support for such data-sharing: 82.1 percent of the South Indian respondents; 73.7 percent of East; 51.7 percent of West; and 38.2 percent of North.

[127] Results of the test of significance for difference of proportions in large samples: Z score = 2.1991, p-value = 0.0278

Do you think hospitals and banks should make it easy for you to digitally share your medical or financial history with a new doctor or a financial advisor of your choice?



A majority of males (56 percent) and of female respondents (52–56 percent) support data-sharing to empower data principals. On disaggregating responses in this context simultaneously by gender and region, the gender divergences in responses is notable especially for North India, South India, and West India, though the direction of divergence is not uniform. While in North India, a higher proportion of males (42.7 percent) support data-sharing to empower data principals compared to the proportion of females (31.3 percent), the proportion is higher for females in the three other regions. The proportions of female respondents supporting data-sharing to empower data principals are: 54 percent for West, 78.5 percent for South, and 84.5 percent for East. For the males, the proportions are: 42.4 percent for West, 69.7 percent for South, and 80 percent for East. In the context of this question, gender deviations in responses are statistically significant at the five-percent level of significance for both North and West India.[128]

[128] Results of the test of significance for difference of proportions in large samples:
North India : Z score = 2.5227, p-value = 0.01174
West India : Z score = 2.3214, p-value = 0.02034

A conservative majority of both Gen-Z (52–53 percent) and millennial respondents (55–59 percent) support data-sharing to empower consumers. About 59 percent of the millennial and 52 percent of the Gen-Z respondents support hospitals and banks sharing citizens' medical or financial history with a new doctor or a financial adviser of their choice. The divergence is statistically significant at the five-percent level of significance.[129] Similarly, a conservative majority of those with a higher level of education (56 percent) and those with a lower level of education (52–55 percent) support this proposition. Across employment status, 58.3 percent of those employed and 53.7 percent of the unemployed, believe that hospitals and banks should digitally share citizens' medical or financial history with a new doctor or a financial adviser of their choice.[130]

D. Survey Responses and SDGs, Human Development Indices

This section makes an assessment of the interrelationships between the perceptions and preferences of respondents from different regions, on one hand, and on the other, the regional scores for the Sustainable Development Goals (SDGs) and the Human Development Index (HDI).

Table 1: SDG Score (2020-21) and HDI Score (2019), by Region

Region	SDG Score	HDI score
South India	71.14	0.711
West India	70.3	0.701
North India	65.07	0.669
East India	63.2	0.657

*Sources: NITI Aayog SDG India Index*131*, Global Data Lab*132 *and author's calculation*133

[129] Results of the test of significance for difference of proportions in large samples: Z score = 3.071, p-value = 0.00214

[130] Results of the test of significance for difference of proportions in large samples: Z score = 2.0715, p-value = 0.03846

[131] NITI Aayog, Government of India, SDG INDIA Index & Dashboard 2020-21: Partnerships in the Decade of Action, 2021 https://www.niti.gov.in/writereaddata/files/SDG_3.0_Final_04.03.2021_Web_Spreads.pdf.

[132] Global Data Lab, Sub-National HDI 2019: India. Human Development Indices (5.0), https://globaldatalab.org/shdi/maps/shdi/?zoomto=IND.

[133] The SDG and HDI scores for the four regions are calculated as the arithmetic mean of the scores of the states belonging to those regions.

Table 1 shows that South India is the top performer in both SDG and HDI scores, followed by West, North, and East India.

In this section, the authors assess the interaction between the responses on the questions related to *individual privacy* and *economic well-being,* on one hand, and on the other, the regional SDG and HDI scores. In the present exercise, the authors compare the trends in response behaviour of the average respondents belonging to different regions with the patterns in regional SDG and HDI indices. The focus is on the issues of *individual privacy* and *economic well-being.*

For the question of *individual privacy,* in order to compute the response behaviour of an average respondent from each region, the proportion of responses in which each respondent in a given region has extended support for the value of individual privacy is determined. An average of this proportion is then calculated across all the respondents belonging to the region under consideration. This average can be interpreted as how likely an average respondent of a given region is to choose in *favour of,* than *against individual privacy.* Such an exercise is conducted for all regions. The exercise is also undertaken for the issue of *economic well-being:* the averages thus computed can be interpreted as how likely an average respondent of a given region is to choose in favour of economic well-being than against it.

Table 2: Mapping individual responses on individual privacy and economic well-being, by Region

Region	Response behaviour of an average respondent in the case of:	
	Individual privacy	Economic well-being
East India	0.71	0.82
South India	0.69	0.81
West India	0.68	0.72
North India	0.62	0.71

The objective of ‘inclusive development’—i.e., “leaving no one behind”—across all domains including technology, underpins the achievement of the SDGs. Higher levels of human development are compatible with the expansion of the freedoms and choices that can be enjoyed by individuals. Therefore, it can be theorised that higher SDG and HDI scores are compatible with greater awareness of rights and responsibilities associated with individual privacy and economic well-being. An average respondent from a region with higher SDGs and HDI scores is more likely to choose in favour of, than against individual privacy and economic well-being.

At the same time, the authors were confronted with counterintuitive theories: for example, the average respondent from East India is most likely to choose in favour of, than against both individual privacy and economic well-being as compared to other regions despite recording the lowest scores on SDGs and HDI. This could be explained using the following reasoning: East India has the lowest mobile connectivity with 81 mobile connections per 100 persons, which is below the national average of 84 mobile connections per 100 persons. Furthermore, East India has the highest income inequality with about 43.46 percent of its population in the lowest two wealth quintiles, again higher than the national average of 40 percent. It could be the case that the ownership of mobile connections is also significantly skewed in the population, with the economically better-off (and gaining more benefits from development) owning more connections than the economically worse-off (and benefiting less from development). Since the population from which the sample is drawn is of those who own mobile connections, the sample may not be representative of the total population. Due to the aforementioned skewness in the ownership of mobile connections in favour of the economically better-off, it appears that the chosen sample is aware of its rights and responsibilities vis-à-vis the technology space and actively enjoys and executes those rights and responsibilities.

As far as the other regions are concerned, the results are as expected. As can be seen, the average respondent of a region with a higher SDG and HDI score is more likely to choose in favour of, than against individual privacy and economic well-being.

E. The Digital 'Trilemma': Digital Privacy, National Sovereignty and Security, and Economic Well-Being

a) Overall responses on individual privacy, national sovereignty and security, and economic well-being

This report hypothesises that an irreconcilable trinity exists in the choices being made by India's youth in relation to individual privacy, national sovereignty and security, and economic well-being. More specifically, it is hypothesised that the youth tend to choose in favour of two of these considerations while inevitably neglecting the third.[134] This so-called "digital trilemma" for reconciling the three values has highlighted challenges in policymaking as well.[135] This section investigates whether or not such a digital trilemma is reflected in the overall responses to the survey. In order to assess whether the dilemma does manifest in the aggregation of the responses to the survey, the authors classified the questions as belonging to one of the three parameters— individual privacy, national sovereignty and security, and economic well-being.

[134] Ariel Kastner, 7 Views how technology will shape geopolitics, *World Economic Forum*, April 7, 2021. https://www.weforum.org/agenda/2021/04/seven-business-leaders-on-how-technology-will-shape-geopolitics/.

[135] Samir Saran, "Our Common Digital Future" *Observer Research Foundation,* (2021) https://www.researchgate.net/publication/332752678_OUR_COMMON_DIGITAL_FUTURE.

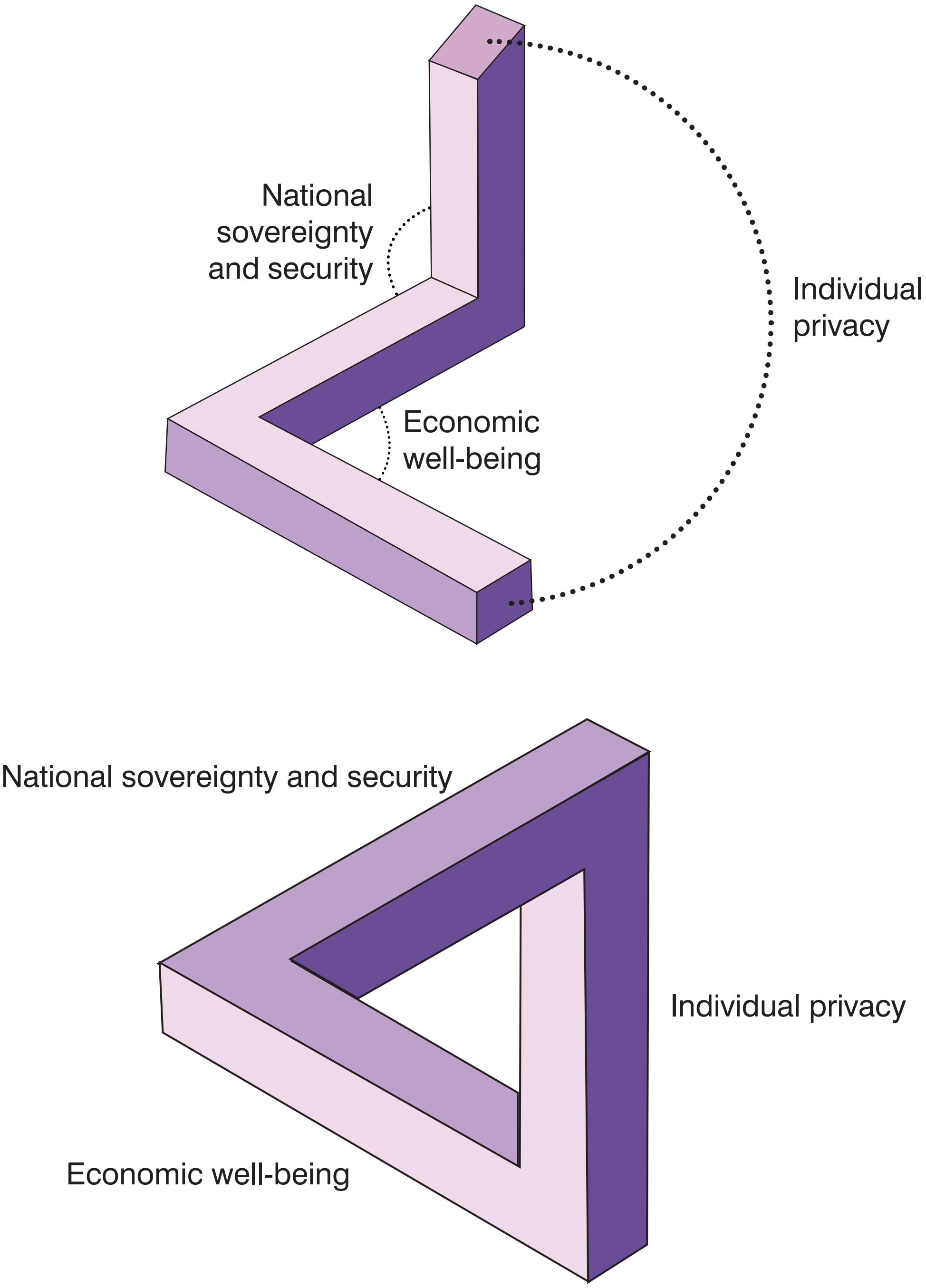
Within each parameter, the authors then compute for each respondent the proportion of responses in which that respondent has chosen in favour of, than against the value associated with the consideration related to the parameter. For example, in the case of the parameter of individual privacy, for each respondent, the proportion of responses in which that respondent has chosen to value individual privacy is computed. An average of this proportion is then calculated across all the respondents to the survey. This exercise is conducted for all three parameters.[136] These averages can be interpreted as how likely an average respondent is to choose in favour of, than against a given consideration. For example, for the national sovereignty and security parameter, the average is interpreted as the likelihood of the average respondent choosing in favour of national security than against it.

Since these "likelihoods" can be translated as averages of proportions, their value lies in the interval [0,1]. The likelihood of an average respondent choosing in favour of individual privacy is 0.62, while that of choosing in favour of national sovereignty and security is 0.76, and that of favouring economic well-being is 0.75.[137] An average respondent appears to exhibit a greater likelihood of choosing in favour of national sovereignty and security than against it, as compared to the likelihood of choosing in favour of individual privacy than against it. The difference between these likelihoods is 0.14.

[136] Averages of the proportions across the three parameters (individual privacy, national security and sovereignty, and economic well-being), are 0.6223032128, 0.7646491087, and 0.7485663496 respectively.

[137] Averages of the proportions across the three parameters (individual privacy, national security and sovereignty, and economic well-being), are 0.6223032128, 0.7646491087, and 0.7485663496 respectively.

Figure 2: Penrose triangle (digital trilemma) for overall responses



The statistical significance of this difference is examined using the difference of means test for large samples. This difference turns out to be statistically significant at the one-percent level of significance.[138] This corroborates the claim that an average respondent exhibits a greater likelihood of choosing in favour of national sovereignty and security than against it, as compared to the likelihood of choosing in favour of individual privacy than against it. Using the same method, it is corroborated that an average respondent exhibits a greater likelihood of choosing in favour of economic well-being than against it, as compared to the likelihood of choosing in favour of individual privacy than against it—with the difference in likelihoods being 0.13.

The difference of means test for large samples suggests that the difference of 0.01 between the likelihood of choosing in favour of national security than against it, and that of choosing in favour of economic well-being than against it, is statistically significant. However, it must be remembered that this result is a statistical artefact following from a large sample size, which allows even minor differences to be detected statistically. Substantively speaking, though, the difference of 0.01 is insignificant. In other words, the likelihood of choosing in favour of national sovereignty and security than against it, is the same as the likelihood of choosing in favour of economic well-being rather than against, at around 75 percent.

[138] Results of difference of means test for large sample :

1. Individual privacy and national sovereignty & security : $(X2-X1)/\sqrt{[(S1/N1) + (S2/N2)]} = (0.7646491087-0.6223032128)/\sqrt{(0.0000170145+0.00002107441)} = 0.1423458959/0.00617162134 = 23.0645867687$ (values are statistically significantly different).
2. National sovereignty & security and economic well-being : $(X2-X3)/\sqrt{[(S2/N2) + (S3/N3)]} = (0.7646491087-0.7485663496)/\sqrt{(0.00002107441+0.00001258976)} = 0.0160827591/0.00580208324 = 2.77189389306$ (values are statistically significantly different)
3. Individual privacy and economic well-being : $(X3-X1)/\sqrt{[(S1/N1) + (S3/N3)]} = (0.7485663496-0.6223032128)/\sqrt{(0.0000170145+0.00001258976)} = 0.1262631368/0.00544097969 = 23.2059562788$ (values are statistically significantly different).

These results suggest that an average respondent is more likely to choose in favour of national sovereignty and security, and economic well-being, than against, as compared to choosing individual privacy than against it. The choices inherent in the responses to the survey do exhibit the digital trilemma in a probabilistic sense.

b) Specific responses on individual privacy, national sovereignty and security, and economic well-being

The authors appraised responses to three questions in the survey that gauge respondents' views on protectionist policies for the broader technology industry in the context of individual privacy, national sovereignty and security, and economic well-being.

- Individual privacy: "How often do you prefer to use Indian social media applications like Josh, Koo, Chingari and so on in comparison to foreign social media applications like Whatsapp, Twitter, Facebook and so on?"
- National sovereignty and security: "Should India adopt protectionist measures to ensure its domestic technology industry is internationally competitive?"
- Economic well-being: "Do you support the Indian government investing in the development of social media platforms in indigenous languages and for local communities?"

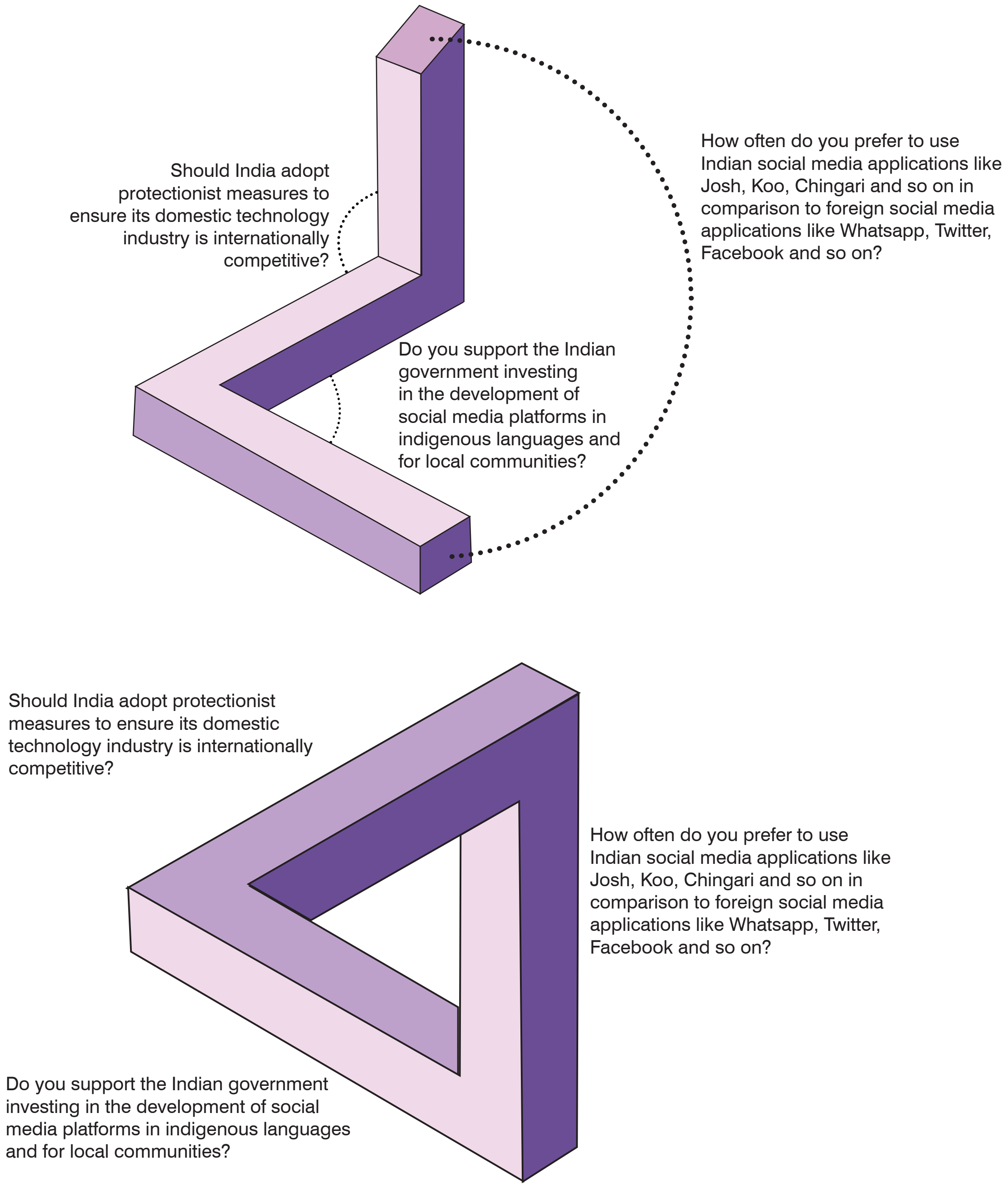
Among those who do not choose to use Indian social media platforms over foreign ones, 84.2 percent agree that India should adopt protectionist measures to make its domestic technology industry internationally competitive. Similarly, among the respondents who do not choose Indian social media platforms over foreign ones, 89 percent support the development of social media platforms in indigenous languages and for local communities.

Employing the test of significance for a single proportion for large samples, the authors have established that both the percentages of responses—i.e., 84.2 percent and 89 percent—are statistically significantly greater than 50 percent. Thus, a statistically significant majority of those who do not choose Indian social media platforms over foreign ones also favour protectionism for an internationally competitive domestic technology industry, and the development of social media platforms in indigenous languages and for local communities.

It follows that among those who favour foreign social media platforms over Indian ones, 15.8 percent are against protectionist measures for the domestic technology industry, and 11 percent do not support developing social media platforms in indigenous languages and for local communities. The authors assume the worst-case scenario that all of the 15.8 percent of respondents against protectionist measures for the domestic technology industry belong to the 89 percent of those who support the development of social media platforms in indigenous languages and for local communities.

Similarly, the authors also assume that all of the 11 percent of respondents who do not support developing social media platforms in indigenous languages and for local communities belong to the 84.2 percent who choose in favour of India adopting protectionist measures to make its domestic technology industry internationally competitive.

Figure 3: Penrose triangle (digital trilemma) for specific responses


Should India adopt protectionist measures to ensure its domestic technology industry is internationally competitive?
How often do you prefer to use Indian social media applications like Josh, Koo, Chingari and so on in comparison to foreign social media applications like Whatsapp, Twitter, Facebook and so on?
Do you support the Indian government investing in the development of social media platforms in indigenous languages and for local communities?
Should India adopt protectionist measures to ensure its domestic technology industry is internationally competitive?
How often do you prefer to use Indian social media applications like Josh, Koo, Chingari and so on in comparison to foreign social media applications like Whatsapp, Twitter, Facebook and so on?
Do you support the Indian government investing in the development of social media platforms in indigenous languages and for local communities?

Accounting for these assumptions, it follows that a minimum of 73.2 percent of those who favour foreign social media platforms over Indian ones simultaneously support protectionism for an internationally competitive domestic technology industry, as well as developing social media platforms in indigenous languages and for local communities. Based on the test of significance of a single proportion for large samples, the authors conclude that 73.2 percent is statistically significantly greater than 50 percent. A significant majority of the respondents who do not choose Indian social media platforms over foreign ones, support protectionism in the contexts of national sovereignty and security, and economic well-being, while choosing against protectionism in relation to individual privacy. This is an instance of the irreconcilable trinity playing out in the set of choices for India's youth.

SCOPE FOR FUTURE RESEARCH

This survey generated noteworthy findings regarding how well the youth of India understand policy debates around issues related to technology that have ramifications in their everyday lives. It creates a path for other, more detailed research in the future on why those surveyed responded the way they did. For example, respondents from the Eastern states of the country generally have an unconventionally significant understanding of issues about individual privacy, national sovereignty and security, and economic well-being. More of these respondents also expressed support for giving priority to national sovereignty and security concerns in the cyber realm, over individual privacy or economic well-being. Future research could explore the behaviour of respondents from East India in cyberspace and the spillover impacts of national security concerns on individual privacy.

In an era witnessing a slowdown in globalisation amidst trade wars and COVID-19-induced restrictions on the movement of people and goods, it is worth reiterating that India's youth support the country's participation in international collaborative measures to ensure cybersecurity. This finding could serve as a springboard for future research on the impacts of new technologies like AI on privacy, and the role India can play in multilateral institutions that work on mitigating these impacts.

Future research may also look at gender- and education-related deviations in responses concerning data hygiene habits. The results of the present analysis have indicated that respondents who identify as females, and respondents with lower levels of education, are less meticulous in data hygiene. Future research on the subject can consider the findings of the present research as the basis to evaluate the efficacy of data literacy programmes targeted towards females, school students, and those who have received little or no formal education.

This investigation into whether an impossible triangle exists in the views of young India related to individual privacy, national sovereignty and security, and economic well-being needs to be scaled up: Can the trilemma be resolved? While the youth respondents prefer data localisation and the adoption of protectionist policies for homegrown tech companies, they are less keen on using Indian alternatives to social media and e-commerce—this implies contradictory choices. It would be interesting to unearth more such contradictions and explain why they exist, and to investigate whether a resolution to the Penrose triangle as established in this report is possible in technology policy. Future research could also broaden the sample to include rural populations, individuals who identify as non-binary or transgender, and other populations of interest.

CONCLUSION: PRACTICES, POLICIES, AND INVESTMENTS

As the world required innovative solutions to the cascading impacts of the COVID-19 pandemic, many of the response measures that delivered results rode on the back of technology: distance learning;[139] contact-tracing;[140] drug and vaccine development;[141] disseminating COVID-19 protocols and monitoring compliance;[142] and remote work.[143] While the acceleration of digitisation helped keep economies from completely shutting down, it also provoked concerns around data-sharing and value-generation and, in turn, issues of data ownership, data protection and privacy, and misuse of collected data by state and private entities.

ORF's technology policy survey, *Swiping Right on Tech Policy,* was designed to understand the perceptions and attitudes of India's youth around these concerns. The findings from the survey offer insights into how the youth understand and relate

[139] Larry Dignan, "Online learning gets its moment due to the COVID-19 pandemic: Here's how education will change," *ZDNet*, March 23, 2020, https://www.zdnet.com/article/online-learning-gets-its-moment-due-to-covid-19-pandemic-heres-how-education-will-change/.

[140] Dyani Lewis, "Contact-tracing apps help reduce COVID-19 infections, data suggest," *Nature* (2021) https://www.nature.com/articles/d41586-021-00451-y.

[141] OECD, *Using artificial intelligence to help combat COVID-19,* 2020, https://www.oecd.org/coronavirus/policy-responses/using-artificial-intelligence-to-help-combat-covid-19-ae4c5c21/

[142] "Drone surveillance to monitor COVID protocol violations in Delhi", *The New Indian Express*, April 26, 2021, https://www.newindianexpress.com/cities/kochi/2021/apr/26/drone-surveillance-to-monitor-covid-protocol-violations-in-kochi-2294791.html.

[143] OECD. *Teleworking in the COVID-19 pandemic: Trends and prospects,* 2021,https://www.oecd.org/coronavirus/policy-responses/teleworking-in-the-covid-19-pandemic-trends-and-prospects-72a416b6/.

to the role of technology in their lives. The study also measures their support for interventions related to the regulation of data and technology across three parameters: individual privacy, national sovereignty and security, and economic well-being.

The youth of India, as represented by the respondents, demonstrate a significant understanding of privacy and related cyber-hygiene practices that keep data safe. From keeping strong passwords to reading privacy policies, individuals ascribe values to the efforts they make to secure their individual privacy. They also demand that the government and the private tech players allow users a voice in how their data is shared, and respect their right to be forgotten. These concerns run parallel to the principles underlying the consent framework as well as the notion of third-party data intermediaries outlined by the Indian government.

The survey respondents—irrespective of age, gender, education, employment status, and region—expressed a significant degree of support for international collaboration that will address the emerging challenges to privacy and security emanating from novel technologies like AI. Support was also declared for mitigating cybercrimes through the implementation of deterrence mechanisms in the form of fines and economic sanctions. Respondents largely showed a strong inclination towards data localisation, tech protectionism, and channelling investments in offensive cyber capabilities. They also demanded that governments put into place statutes that will ensure more transparency and accountability from foreign social media companies.

In data-sharing for rations and law enforcement—where there are value trade-offs between individual privacy on the one hand, and on the other, economic well-being and national sovereignty and security— respondents largely favour the latter two. There is greater support for immediate concerns such as ensuring road safety, as compared to long-term ones like assisting in anti-terrorism efforts, or reducing cybercrimes and foreign interference in elections.

Indeed, it is not only the youth of India who have strong opinions about the behaviour of governments and companies in the domain of technology. For example, Deloitte's Global 2021 Millennial and Gen-Z survey[144] found that in the time of COVID-19, the youth have become more resolute in bringing change into how systems function and in demanding for accountability from the government and private enterprises.

For its part, the November 2021 survey, "Future of Digital Spaces and Their Roles in Democracy" by Pew Research Center and Elon University found that governments have to exercise "soft" pressure on social media companies to address issues that involve their platforms. The February 2021 global survey by EY also highlighted the anxieties of individuals related to the privacy and security of data collected by governments and private enterprises. It found that individuals would be willing to share their data with the government if they have been informed of its use, and if such data-sharing offers benefits to society. Meanwhile, the 2021 survey by *Washington Post* and the Schar School of Policy and Government at George Mason University has also suggested that individuals are less likely to trust that social media platforms will handle information or data generated about consumers in a responsible manner.

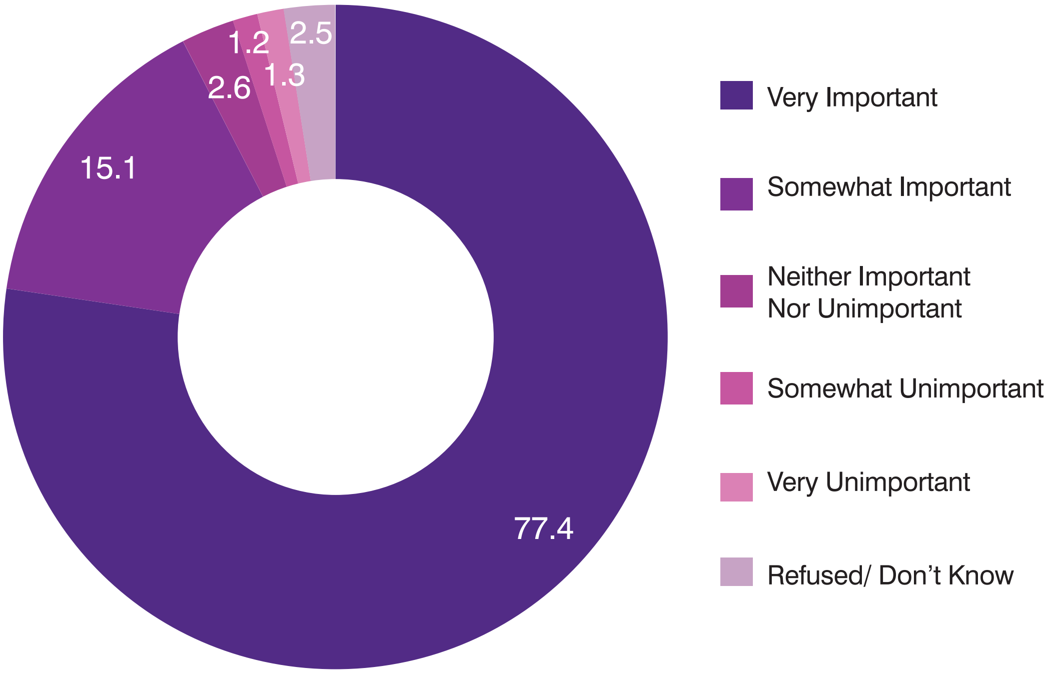
[144] Deloitte, The Deloitte Global 2021 Millennial and Gen Z Survey, 2021, https://www2.deloitte.com/global/en/pages/about-deloitte/articles/millennialsurvey.html

This present survey offers the following recommendations.

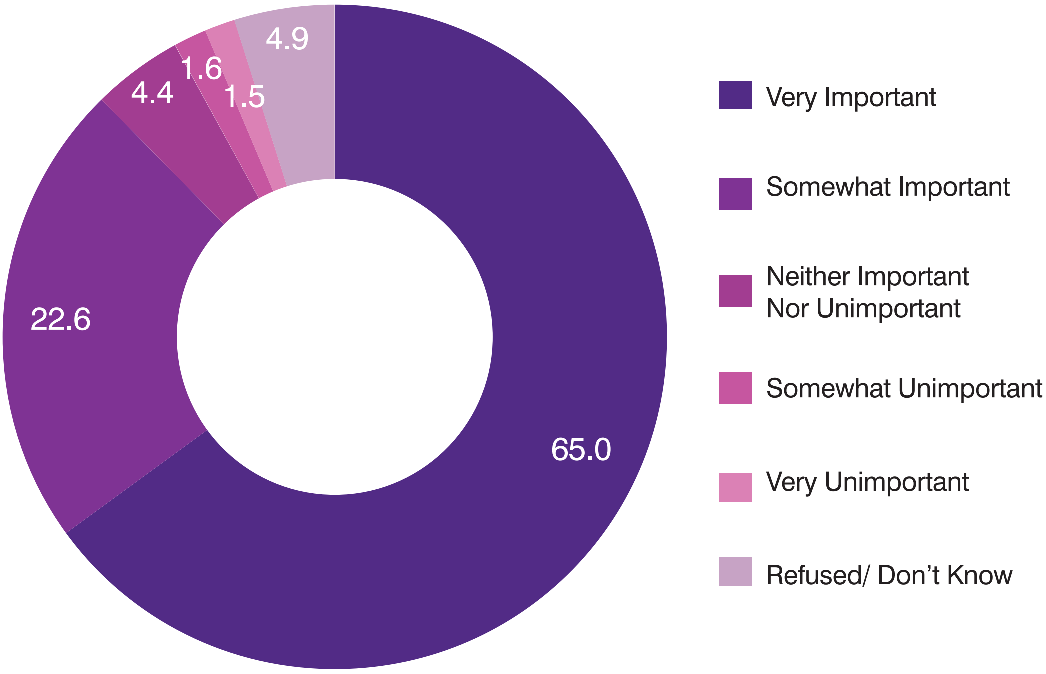
1. A significant majority of India's youth support government investments in critical supply-side aspects of the country's technological growth. This is consistent with the findings of the 2020 survey conducted by the Office of the Principal Scientific Adviser to the Government of India and the IIT Madras Alumni Association, in which respondents stated that, one, India should prioritise economic growth and job creation in the pandemic era, and two, that within the nation's technology domain, attention should be paid to Information Technology.

   The present survey found that 92 percent of the respondents supported investment in infrastructure such as mobile towers to ensure internet connectivity across the country. Eighty-eight percent of respondents support investment in the development of an open data regime that enables innovation in AI, an uninterrupted supply of critical mineral resources for batteries for electric vehicles, alternatives to foreign social media or encrypted messaging platforms that cater to local communities and vernacular languages, and domestic manufacturing capacity for indigenous computers or mobile chips. In this context, the government must aim to strike a balance between self-reliance in the domain of technology, and technology protectionism. This is also important to avoid derailing the growth of the services sector, which has proved to be an engine of growth over the past two or so decades.

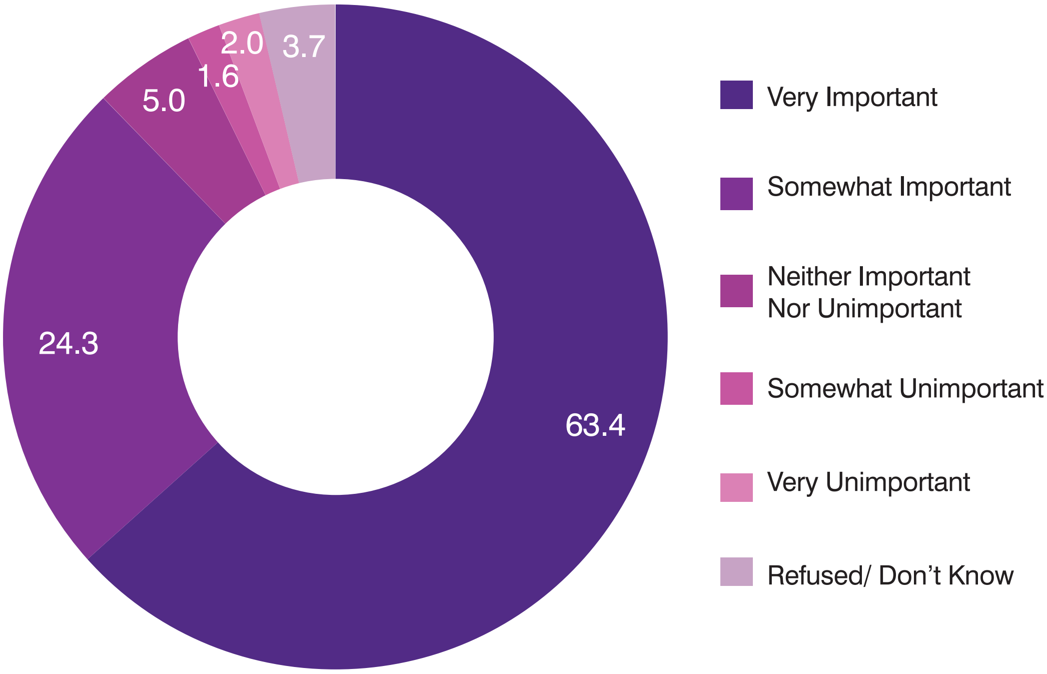
Do you support the Indian government investing in the development of infrastructure like mobile towers to ensure internet connectivity across the country?



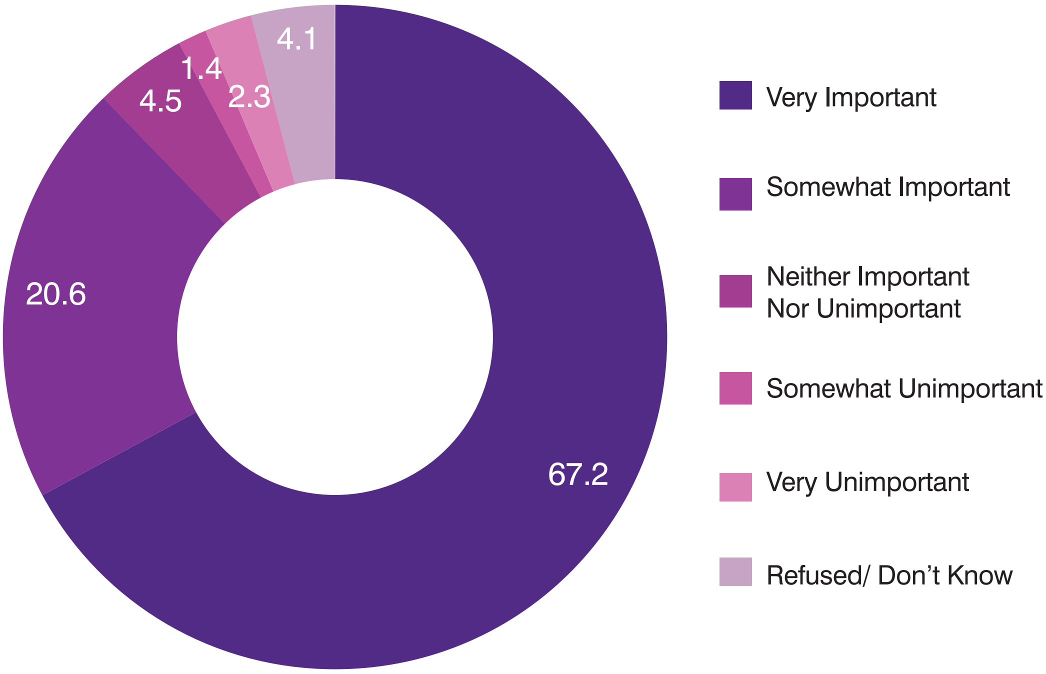
Do you support the Indian government investing in the development of an open data regime that enables technological innovation by ensuring increased and standardised access to data?



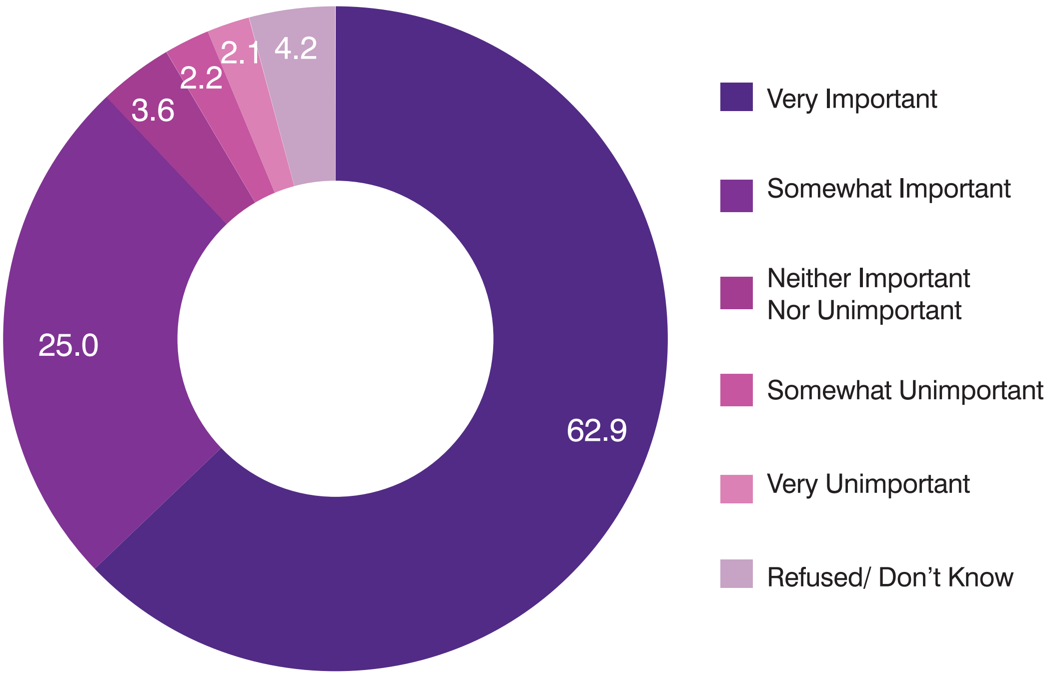
Do you support the Indian government investing in the promotion of the continued supply of critical mineral resources that go into making batteries for electric vehicles?



Do you support the Indian government investing in the development of indigenous computer or mobile chips?



Do you support the Indian government investing in the development of social media platforms in indigenous languages and for local communities?



2. India’s youth have little trust that foreign companies and social media platforms will work to ensure their privacy. A majority of the respondents support the idea that between local and foreign companies that violate privacy laws, the latter should be meted higher fines. They also agree to fines on social media companies that allow the misuse of their platforms. This lack of trust aligns with the demand for redesigning online spaces, which is being repeated by citizens in other parts of the world, such as the US and Europe. At the same time, while this demand for higher fines on foreign enterprises could act as a deterrent against violations of privacy, it needs to be refined to obligate platforms to disclose data breaches. Both the JPC report and the Draft Data Protection Bill 2021 mandate data fiduciaries[145]

[145] Data fiduciary is the entity or individual responsible for deciding the purpose and means of processing personal data.

to inform the Data Protection Authority about a data breach under Clause 25. Moreover, in the context of imposing fines on social media platforms for their misuse, there is a need to develop clear standards and rules, in order to ensure that dissent is not censured.

More than four of every 10 respondents (42.5 percent) are willing to use local social media and e-commerce platforms. A greater proportion of users in India might start using local platforms more often if they can be convinced that these companies engage in due-diligence measures for data safety and privacy. Additionally, considering that the dominant mode of communication is English on most social media platforms, local social media platforms could perhaps attract users by providing similar services in vernacular languages. With 62.4 percent of millennials stating their willingness to try local social media platforms, this is a positive signal for these companies to widen their user base.

3. A majority of respondents stated their willingness to share personal data with government and private sector enterprises to assist in addressing national security and law enforcement concerns. However, respondents did not concede to a blanket sharing of their data; rather, only to meet specific purposes. Both the public and private sectors must be mandated to practice transparency in their data collection, and to abide by cybersecurity protocols.

4. The demand for responsible models of data-sharing that ensure gains not just for the individual but also for society is evident from among respondents across different demographic cohorts. The Government of India and the private sector engaged in developing and deploying public service delivery systems must explore possibilities for reconciling the digital trilemma for data-sharing. The alternative model for data-sharing must ensure user-centricity, data interoperability, granular control by citizens, and compliance with existing laws. While the government has proposed certain policies like DEPA to enhance user's control of their data, these are yet to acquire widespread public support. Information about such proposals have to be disseminated to the larger public as part of digital literacy strategies.

5. The divergence in the practice of cyber hygiene among respondents across regions, gender, education, and employment status calls attention to the need for data literacy and cyber hygiene programmes with different stakeholders. For instance, initiatives like the 'Digital Literacy and Online Safety Programme'[146] launched in 2018 by the National Commission for Women, Facebook, and CyberPeace Foundation, could be expanded to include more stakeholders such as other non-government organisations and civil society organisations. There should be a specific focus on females and unemployed youth, considering the divergences in their responses.

6. The government-run Common Service Centres have been offering free online cybersecurity courses since 2020 under the 'Digital India' and 'Transforming India' campaigns, with the aim of increasing awareness on cybersecurity-related matters among school students.[147] The divergence on the dimension of education and the importance of ensuring digital literacy calls for such programmes to be scaled up, to make school students aware of data hygiene and online safety.

7. A majority of the respondents irrespective of gender, age, level of education, and status of employment agree that the private sector should channel greater investments in data localisation. To that end, the JPC Report has initiated the process of developing comprehensive data localisation standards. These standards must attempt to draw a balance between 'hard' and 'soft' forms of data localisation, wherein the former implies no cross-border storage or processing while the latter allows for some degree of both, which is essential for the growth and sustenance of a 'global village' impacting the start-up ecosystem in India.[148]

[146] National Commission for Women. "Digital Literacy and Online Safety Programme." (June 2018). http://ncw.nic.in/basic-page/digital-literacy-and-online-safety-programme.

[147] Digital India, Government of India. *CSC offers a free online course in cybersecurity for students,* 2020, https://digitalindia.gov.in/content/csc-offers-free-online-course-cybersecurity-students.

[148] Ajay Patri, "Hard and Soft Data Localisation." Pragati Express, August 4, 2018, https://express.thinkpragati.com/2018/08/04/hard-and-soft-data-localisation/.

8. India must continue to engage in bilateral and multilateral partnerships to address the risks emanating from AI and other higher-tech innovations. These collaborations should also deal with threats such as foreign interference in domestic elections, and hacking campaigns against critical public infrastructure. These engagements can assist India in enhancing its technological and cyber security capabilities in order to implement its National Programme on AI and the revised National Cybersecurity Strategy.

ABOUT THE AUTHORS

Antara Vats is a Junior Fellow at ORF, Delhi.

Anushka Saxena is a Research Intern at ORF, Delhi.

Dr Renita D'Souza is a Fellow at ORF, Mumbai.

Acknowledgements

Dr. Samir Saran, Dr. Nilanjan Ghosh and Dr. Rajeswari Rajagopalan, for their guidance, support and invaluable suggestions in strengthening this report and bringing it to fruition.

Akshay Mathur, for his valuable inputs.

Trisha Ray, Samyak Rai Leekha, Saranya and the entire team of the Centre for Security, Strategy and Technology at ORF Delhi, for their inputs in designing the study and the questionnaire.

Kamya Chandra, Siddharth Shetty, and Arun Mohan Sukumar, for their inputs and suggestions in making a sharper questionnaire.

Impetus Research, for administering the study in an efficient manner.

ANNEXURE

1. How often do you keep strong passwords with uppercase letters, lowercase letters, numbers and special characters?
2. How often do you clear your browsing data?
3. How often do you keep different passwords for different accounts?
4. How often do you keep your passwords confidential?
5. How often do you enable two level authentication on your devices?
6. How often do you update your software?
7. How often do you read privacy policy before registering on any application?
8. How often do you allow limited access to sensitive data like photos, location and contacts to a new application that you download on your phone?
9. How often do you use a VPN?
10. How often do you use privacy settings on social media to restrict access to personal information?
11. How often do you use Indian social media applications like Josh, Koo, Chingari and so on in comparison to foreign social media applications like Whatsapp, Twitter, Facebook and so on?
12. How often do you think e-commerce websites share your personal information including information on last searched item with social media platforms to show relevant product advertisements to you?

13. Do you think independent establishments could assist in simplifying the process of sharing your personal details and physical documents like signatures, property papers, and details of previous loans to banks when applying for new loans to make the process of data sharing easier?
14. Do you support countries cooperating with each other to minimise privacy and security risks which are arising out of newer technologies like AI?
15. Do you think that you should have a say in how your data, for instance, browsing data, transaction history, and profile held by institutions such as social media companies, banks, government departments, hospitals/doctors, and mobile apps is shared?
16. Would you be comfortable selling your biometric data like eye or fingerprint scan in exchange for INR700?
17. Would you be comfortable sharing your personal data like location data to assist the government in conducting anti-terrorism efforts?
18. Would you be comfortable sharing your personal data like location data to assist the government in stopping foreign interference in Indian elections?
19. Would you be comfortable sharing your personal data like financial data to assist the government in reducing organised cybercrimes like financial frauds, hacking and ransomware attacks?
20. Would you be comfortable sharing your personal data like location data to assist the government in ensuring road safety?
21. Would you be comfortable sharing your personal data like medical records to assist the government in avoiding public health emergencies by maintaining a robust healthcare record for national health insurances?
22. Would you be comfortable sharing your personal data like financial records to assist the government in providing ration or cash to the weaker sections of the society?
23. Do you think hospitals and banks should make it easy for you to digitally share your medical or financial history with a new doctor or a financial advisor of your choice?
24. Do you support the ability of citizens to set limitations on data usage and sharing between companies?

25. Do you support institutionalising a centralised system with a unique ID and password for citizens to verify and update information being saved about them by the government?

26. Would you be comfortable sharing access to the photos on your phone with private companies to track and minimize the distribution and creation of child sexual abuse material on the internet?

27. Are public safety and national security concerns more important for the governments often over individual privacy?

28. Do you support mandatory erasure of user's personal information kept by private companies on the request of the users?

29. Do you support foreign companies being allowed to share personal data generated by Indians with foreign law enforcement agencies to prevent criminal activity on the Internet?

30. Should foreign tech firms localise storing and processing of data generated by Indian citizens?

31. Should India support international coalitions that propose imposing economic sanctions on countries using technology to interfere in foreign elections, for instance, by identifying citizen's voting preferences?

32. Should social media platforms be fined or penalised if their platforms get misused to spread rumours which can potentially challenge your credibility and pose a threat to your job?

33. Should India adopt protectionist measures to ensure its domestic technology industry is internationally competitive?

34. Should the Indian government support the punishing of countries housing cyber-criminal groups under international law as a deterrence to rise in cybercrimes?

35. Should India invest in offensive cyber operations to protect the functionality of its infrastructure projects against nations engaging in electronic or physical warfare as a national security strategy?

36. Should foreign companies violating privacy laws laid down by the Indian government be given harsher punishments e.g., more fines than Indian companies committing similar violations?

37. Do you support the Indian government investing in the development of infrastructure like mobile towers to ensure internet connectivity all across the country?

38. Do you support the Indian government investing in the development of an open data regime that enables technological innovation by ensuring increased and standardised access to data?

39. Do you support the Indian government investing in the promotion of the continued supply of critical mineral resources that go into making batteries for electric vehicles?

40. Do you support the Indian government investing in the development of Indigenous computer or mobile chips?

41. Do you support the Indian government investing in the development of social media platforms in indigenous languages and for local communities?

ORF OBSERVER RESEARCH FOUNDATION

Ideas • Forums • Leadership • Impact

Observer Research Foundation
20, Rouse Avenue Institutional Area
New Delhi - 110 002, INDIA
+91-11-35332000 Fax: +91-11-35332005
contactus@orfonline.org
www.orfonline.org