tsaaro

JUNE 2022

Tsaaro Exclusive Survey Report

PRIVACY AMONG TEENAGERS

TABLE OF CONTENTS

PREFACE

INTRODUCTION

Late adolescence is a crucial period in a child's life when they are growing more independent and autonomous from their parents but are not yet old enough to live independently. Teenagers are also heavy consumers of mobile devices and social media, frequently using them to communicate with friends and share information about their lives. One-third of all internet users are believed to be under the age of 18. Young people come across opportunities and risks online as digital technology progressively mediate practically all aspects of their life, including their education.

Much of the media coverage of young people and online social networks has been centred on the personal information that kids provide on these sites. The concerns for young people online include stumbling across age-inappropriate information, being approached by predators, and being a victim of cyberbullying or cyber abuse. Other, less apparent concerns include economic exploitation via profiling and behavioural advertising, and cultural trends like surveillance normalization, in which young people may get used to being watched and recorded all the time.
Are they disclosing information that might jeopardize their chances of getting into college or landing a job? Or, even worse, are they disclosing information that puts them in danger of being targeted as a victim?
These are a few concerns that need to be addressed to protect children from threats online and to support the development of a healthy, vibrant online ecosystem that is acceptable for teenagers.

WHAT IS DATA PRIVACY?

Data privacy refers to how a piece of information or data should be handled depending on its significance. For example, you probably wouldn't mind revealing your name to a stranger as part of an introduction, but you wouldn't share any further information with that person until you get to know them better. When you open a new bank account, you will most certainly be requested to disclose a great deal of personal information, not limited to your name. In the digital era, we commonly apply the concept of data privacy to the crucial personal statement, also known as personally identifiable information (PII) and personal health information (PHI). Apart from data protection, data availability and accessibility are equally important. Data storage necessitates data management, which includes moving data online and offline, analyzing, safeguarding, categorizing, and securing the data against unauthorized access, virus attacks, disruption, and technical failures.

WHY IS PRIVACY IMPORTANT FOR TEENAGERS?

Teens are increasingly sharing personal information on social media sites, a trend that is likely driven by the evolution of the platforms teens use as well as changing norms around sharing. Teens have a variety of ways to make available or limit access to their personal information on social media sites. Privacy settings are one of many tools in a teen's personal data management arsenal. Teens who are concerned that some of the information they share on social network sites might be accessed by third parties like advertisers or businesses without their knowledge more frequently delete comments, untag themselves from photos or content, and deactivate or delete their entire account. Teens are one age group where privacy is extremely important as at this age teenagers don't really take the time out to read user privacy agreements while signing up on any application and the same can cause a severe privacy breach. Teens all across the world should be educated about privacy to make sure that the data breaches are minimum and that teens are aware of the ways to protect their privacy.

INDIAN LEGAL PROVISIONS

The Information Technology Act, 2000

The Information Technology Act, 2000, being the first legislation on technology, computers, e-commerce and e-communication, incorporates the provisions related to digital data, electronic devices, and cybercrimes. Child abuse has been elaborately dealt with under the broader ambit of Section 67B of the Act. It is further provided that for this section, "children" means a person who has not completed 18 years of age for this section.

Juvenile Justice (Care and Protection of Children) Act, 2015

The Juvenile Justice (Care & Protection of Children) Act, 2015 specifies procedural safeguards in cases of children in conflict with the law and children in need of care and protection. It asserts that data like name, address, school details, or any other information that could lead to identifying the child who is in trouble with the law must not be disclosed or published in any form of media unless it is for the child's best interest.It also states that all reports related to the child shall be treated as confidential.

Draft Data Protection Bill, 2021

Section 16 of the bill lays down the grounds regarding data processing. It states that every fiduciary shall process the data in such a manner that serves the children's best interest, protecting their rights to the children. The Joint Parliamentary Committee (JPC) emphasizes the children's data. It has safeguards like age verification and parental consent before collecting any child's data. Further, the data fiduciaries can't use children's data for any purpose as there are few restrictions on the usage. In contrast to most global regulations, India has mentioned that the age of minorities is below 18.

INTERNATIONAL LEGAL PROVISIONS

General Data Protection Regulation (GDPR)

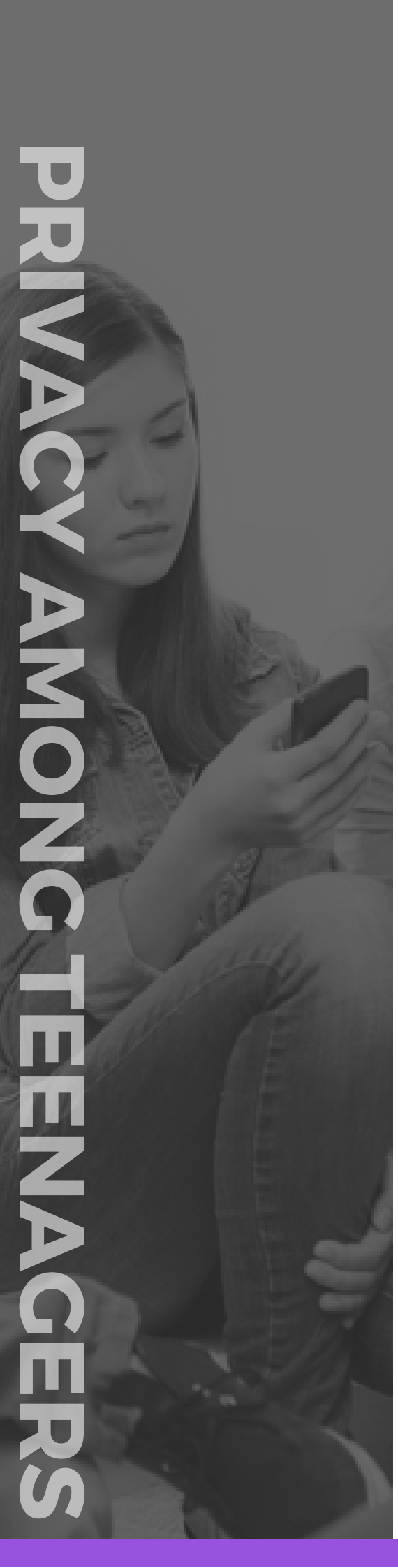
It is a legal framework of the EU that regulates the collection and processing of personal information. General Data Protection Regulation (GDPR) governs the data shared by people with organizations and the safety, privacy, and concerns to be considered regarding the collection and processing of such data. Concerning the right to privacy of children, the provisions of GDPR state that the processing of personal data of a child shall be legal where the child is at least 16 years old. If a child is under 16, the data processing shall be lawful only after obtaining consent or authorized by the holder of parental responsibility for the child.

Cyber Protection of Children's Personal Information

The Cyberspace Administration of China instituted a law called "Digital Protection of Children's Personal Information" for the protection of the online privacy of children. The rule applies to minor children under the age of 14. There are provisions in the Act where the network operators must keep up the righteousness, definite reason, and guaranteed security while gathering, transferring, or unveiling any data.

Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act of 1998 (COPPA) is a U.S. federal law regulating data collection. It aims to protect children's privacy by restricting online websites and commercial services operators from collecting data without parental consent.



SURVEY METHODOLOGY

The survey consisted of 14 questions in a Yes/ No format which aimed at maximizing the number of responses for better insights into the research question. The survey successfully collected the responses of more than 1,000 participants to support the report's claims. The survey was carried out through a Microsoft form where only one response could be recorded from one mail id to protect the authenticity of the responses. The data was then analyzed for the patterns observed amongst the participants.

The purpose of keeping participation in the survey open to all age groups without limiting it to teenagers was to gain better insight by allowing participants to respond about their dear ones. Social media platforms like Facebook, LinkedIn, and Telegram were used to populate the survey, and tie-ups with schools and colleges were made for mass circulation. The survey strictly followed ethical considerations to protect the rights of research participants by providing an option to remain anonymous and maintain the integrity of the research.

THE APROACH

To research and identify privacy among the teenagers and the digital environment they are a part of, this survey prioritizes their experiences within the broader framework of evidence that has been developed by conducting focus group research with different groups, and from selected NGOs around the country. Three search terms were combined (primarily the internet, but including all digital devices, content, and services that an individual can connect to it). Tsaaro sent out the survey to teenagers via different platforms, following a particularly multidisciplinary approach to the research framing and interpretation of results. In order to keep the findings and processes involved in the survey transparent, we have decided to provide the readers with the steps undertaken to conduct this survey. The adjoining flowchart depicts the motive, procedures, and steps taken up by Tsaaro to conduct the survey.

1

RESEARCH

Tsaaro's team studied the Draft DPB, 2021, and IT Act, analyzed various reports on the privacy issues teenagers face, and formulated the questionnaire accordingly.

2

DISTRIBUTE

The survey was sent out to elders and other participants via different platforms to ensure maximum participation.

3

ANALYZE

All the survey participants answered and provided us with their experiences and insights relating to the issue.

4

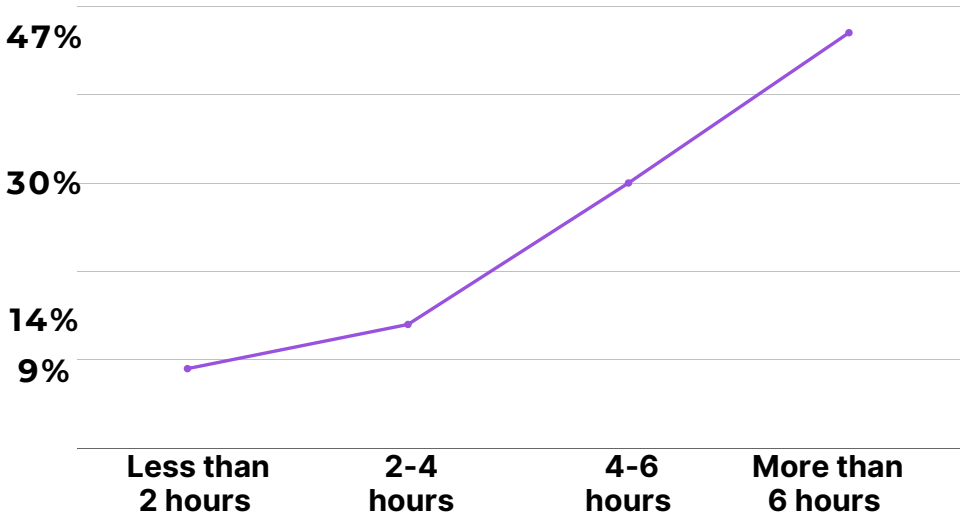
CREATE REPORTS

All the received responses were curated and further presented by Tsaaro in the following report.

SURVEY INSIGHTS

The following inforgrapic depicts the survey results of all the questions asked, along with our comments on the same.

HOW MUCH TIME DO YOU THINK TEENAGERS SPEND ON SOCIAL MEDIA PLATFORMS OR MESSAGING APPLICATIONS?



The privacy risk depends majorly on using platforms where personal data sharing is frequent. The result was an eye-opener wherein many respondents shared that teenagers use such media for more than six hours daily. This raises important questions like whether teenagers know the safeguards they must take to protect their privacy on these platforms.

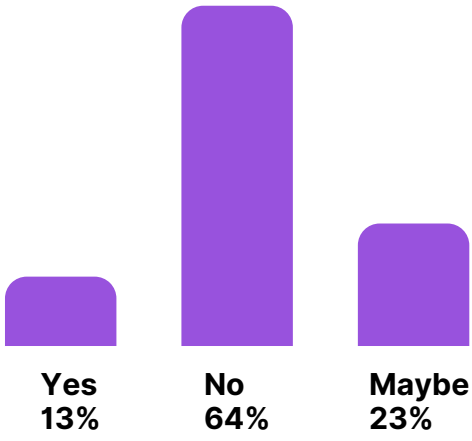
Do you think teenagers end up sharing their personal data online directly/indirectly?

We find ourselves at an inevitable crossroads in this information age; much personal data needs to be shared for various purposes. In that kind of environment, 40% of our participants feel that teenagers share the data online, which may or may not be required to be shared.

47% **of the participants answered that someone who is in teenage in their circle has faced consequences of a privacy breach.**

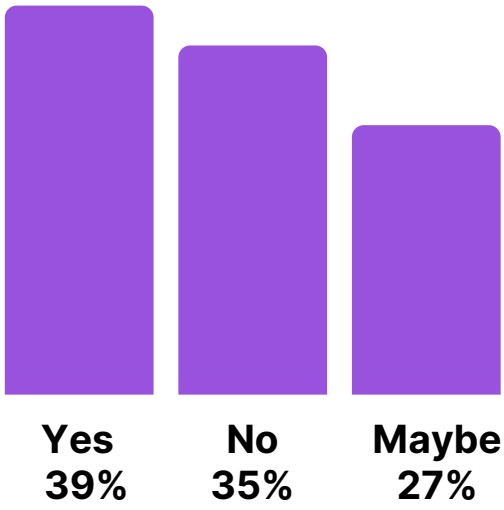
Do you think the teenagers around you are aware of the measures through which they can safeguard their privacy both online and offline?

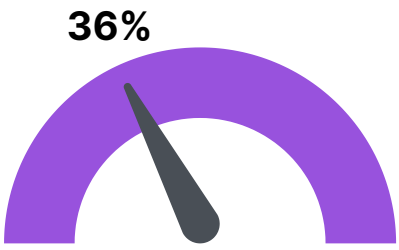
Only 13% of our participants felt that teenagers are aware of the measures that can be used to safeguard their privacy which is a meagre number. It indeed calls for robust steps to be taken to create awareness.



Do you think teenagers are an easy target for fraudulent activities?

39% of our participants felt that teenagers are a soft target for online frauds; this shows that teenagers often cannot keep themselves from all sorts of fraudulent activities. On the other hand, 35% do not consider them an easy target indicating that they can detect when there is some malicious activity taking place. This is a good sign as this shows some teenagers are cautious while using any apps requiring personal information.



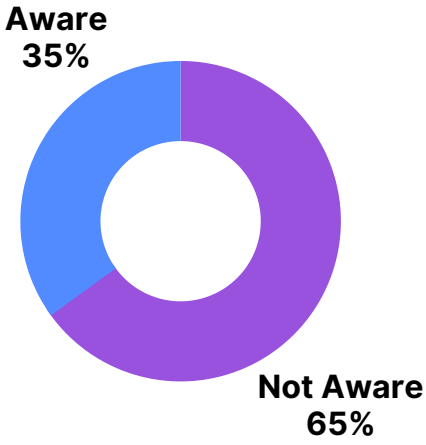


Do you think teenagers take measures for online security (such as identity verification, keeping details confidential etc.) while using the online payment gateways?

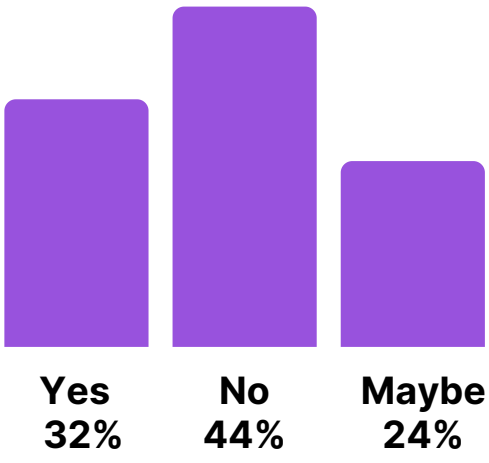
Fast payments at a click are a gateway for huge losses on the other. Most online frauds target financial platforms to enable the unlawful transfer of money, and teenagers, while using such media, should be aware of keeping passwords and OTPs confidential along with limiting the accessibility of their devices. Only 36% of our participants were confident that teenagers take measures for online security in payment gateways.

According to you, are teenagers aware of the risks associated with inputing fake information on social media applications?

Only 35% of our participants feel that teenagers know the consequences of inputting fake information on social media apps. Inputting phoney information can cause problems such as double identities and background checks not coming clean. This may not only cause teenagers issues immediately but also affect them in the long run—for example, identity issues when they apply for college, visas, jobs etc.



Do you think that the features on online platforms (Such as managing access to location, camera, microphone or parental control methods) are enough to safeguard privacy?



Just 32% of the participants believe that features offered by apps to safeguard privacy are enough. This shows that applications need to up their security game to ensure that their users feel safer while using the app, as security is a huge concern. Instead of people installing third-party apps to secure the apps with fingerprint locks, apps should give the option for higher security if the user wants it.

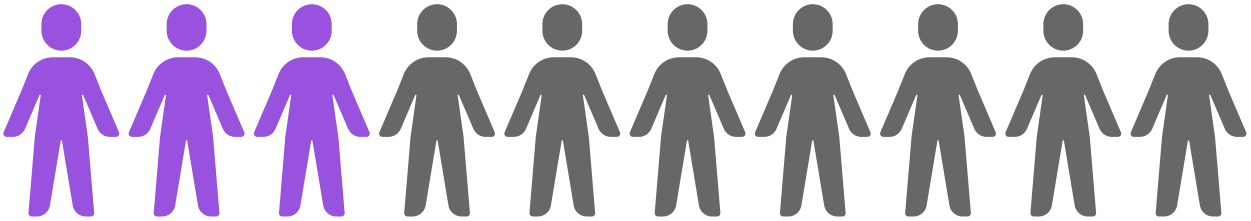
36%

respondents felt that adequate steps were taken

Do you think that adequate steps are taken by parents, schools, colleges and government to make the teenagers aware about privacy?

Just 36% of the participants felt that adequate steps are taken by parents, schools and colleges and the government to make teenagers aware of privacy.

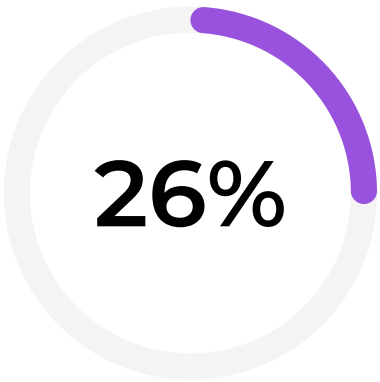
Do you think that the current regulatory framework around privacy laws is enough to enable teenagers to protect their privacy, both online as well as offline?



Only 3 out of 10 participants think the current regulatory framework around privacy laws is enough to enable teenagers to protect their privacy.

Do you think that there is a need for new laws around privacy which will enable teenagers to protect their privacy?

As we can see, 65% of the survey participants have said there is a requirement for new laws. The government should understand that with the current set of rules, most people feel that teenagers cannot protect their privacy. Comprehensive legislation would be the first and the most crucial step towards securing the privacy of the citizens of our country.



SUMMARY

The findings of this survey point toward increasing interest in privacy and a growing concern among participants about the misuse of their data. It indeed is a large issue as only 32% of participants in our survey reported that features offered by apps to safeguard privacy are enough. We saw that 65% of the population felt that there is a need for new laws to help safeguard the privacy of teenagers which is a huge concern, and it is only expected that the government takes steps toward this. Educational Institutes, the government, and parents at home must start educating their teenage children about privacy as only 36% of the participants felt that they are doing enough to educate teenagers about privacy. Addiction to social media is also becoming a very big problem these days and from our survey, we can tell that 47% of the participants feel that teenagers use social media apps for more than 6 hours a day. This is a huge concern for the growing population, one way to decrease time spent time on these apps is to increase awareness among these kids. To conclude, the result of the survey points toward an ever-increasing requirement for better measures that equip teenagers with sufficient knowledge on protecting their privacy and at the same time, better laws to prevent and address the breach of privacy. We at Tsaaro, along with the privacy fraternity of the world, are eager to see what the future of the draft Data Protection Bill, 2021 holds and how it addresses various privacy-related needs.

SUGGESTIONS FOR IMPROVEMENT

We realize that privacy among children is a serious concern, and it must be resolved effectively to make online space a safe place for people across all age groups, especially teenagers. The actors, including the governments, online service providers, educators, and parents, can undertake various steps to assist these efforts.

- **Government:** Governments, corporations, organizations, and other entities that collect, analyze, and exchange the data of young people may create underlying legal protections for responsible data collection and use. Determining the proper age for digital consent, giving consent rights to the parent or kid, supporting a consent-based or rights-based framework, and depending on comprehensive or sector-based law are all significant concerns.

- **Schools:** Schools can use filtering and blocking to highlight and prevent occurrences of self-harm and damage to others, addressing concerns about school safety. Telecommunications firms in nations like South Korea are mandated to prohibit access to content that is harmful to kids.

- **Awareness:** Young people may be empowered through digital literacy and citizenship education and resources to take control of their privacy and encourage informed, appropriate, and responsible online participation.

- **Ban:** For certain age groups, age bands can be used to offer distinct versions of a service or different privacy rights and safeguards. A recent example of using age bands is TikTok's enhanced default privacy settings for users ages 13 to 15, which limit who can comment on, and download videos of users in this age range, as well as turning off the feature that suggests their accounts to others.

Akarsh Singh
(CEO & Co-Founder, Tsaaro)
Akarsh is a fellow in Information Privacy by IAPP, the highest certification in the field of privacy. His expertise lies in Data Privacy and Information Security Compliance.

Krishna Srivastava
(Co-Founder & Head of Cyber Security, Tsaaro)
Krishna is an xKPMG data security consultant. He has vast experience in Information Security and Data Privacy Compliance.

CONTACT US

You can assess risk with respect to personal data and strengthen your data security by contacting Tsaaro.

Tsaaro Netherlands Office
Regus Schiphol Rijk
Beech Avenue 54-62,
Het Poortgebouw,
Amsterdam, 1119 PW, Netherlands
P: +31-686053719

Tsaaro India Office
Manyata Embassy Business Park,
Ground Floor, E1 Block,
Beech Building, Outer RingRoad,
Bangalore- 560045
India

Level 1, Building 10A,
Cyber Hub, DLF Cyber City,
Gurugram, Haryana 122002
India
P: +91-77609-23421

Email us
info@tsaaro.com

ABOUT TSAARO

Tsaaro is a leading data privacy and cyber security service provider helping businesses across technology companies and new-age start-ups secure their applications, through future-ready solutions that help keep up with the changing technology landscape.

Our strength lies in assessing security risks, monitoring for threats, and safeguarding applications against compliance issues as well as the latest threats. We provide data privacy services to align the organization's security roadmap to leading privacy frameworks such as
GDPR, CCPA, PDPB, HIPPA. Our information security services truly complement our capabilities in privacy and security with an exhaustive list of assessment and implementation frameworks such as ISO 27001:2013, NIST, and PCI-DSS.

We take a pragmatic, risk-based approach to provide our clients with real-world, workable advice, guidance, and support that helps them to deal with a wide range of security and privacy-related challenges.