DATA RIGHTS FOR COMMUNITIES

DEF
DIGITAL EMPOWERMENT foundation

Data Rights for Communities

Data Rights for Communities
Early June 2020

Author: Asheef Iqubbal
Editors: Sana Alam and Anulekha Nandi
Concept: Anulekha Nandi
Review: Sana Alam, Shambhavi Madan, Anulekha Nandi, and Osama Manzar
Design and Illustration: Sharada Kerkar

This resource is also available in Hindi: https://bit.ly/2VkcJRP

You can read the online copy at www.defindia.org/publication-2

Published and distributed by:
Digital Empowerment Foundation
House no. 44, 2nd and 3rd Floor (next to Naraina IIT Academy)
Kalu Sarai (near IIT Flyover)
New Delhi – 110016 Tel: 91-11-42233100 / Fax: 91-11-26532787
Email: def@defindia.net | URL: www.defindia.org

The Internet has changed our lives in every possible way-be it our experiences of conversations or expressions of our ideas, beliefs, or even emotions. It has become our livelihood, our source of entertainment, and our mode of release all rolled into one.

However, conveniences come at a cost. The Internet is able to make our lives simpler because it collects our data from every interaction we have with it. How we interact with the Internet tells a lot about our tastes and preference patterns, likes, dis-likes, causes we support, ideas we don't, our spending patterns, our risk profiles, our credit worthiness, whether we are 'model' citizen, or hold opinions that do not toe some imaginary line.

Such data are collected, processed, and used by the entities whose services we use on the Internet. Given how deeply entwined these practices are within our lives, rights we enjoy as citizens and individuals tend to get caught up in how such data are collected and used and how much is revealed to whom and to what extent.

In this context, 'Data Rights For Communities' is an effort to give you a sense of understanding about the data, how it is collected and used, and the rights associated with it.

We all use social media platforms, don't we?

We love sharing photos on different social media platforms. We like looking at pictures of our friends and reacting and comment on them. We also like different pages for different purposes – entertainment, news, gossips, fitness etc. It sometimes feels there is no end to the things we can 'like'.

Have you noticed that while using social media platforms, different advertisements also pop up on our screen, don't they? I have seen them many times and you must have seen them too. Have you ever noticed why only content similar to those that we like keep coming up? I have noticed that whatever I try to search on Google, Amazon, Flipkart, or Paytm, the same advertisements flash on my social media accounts too. You will also notice that something similar happens every time.

Have you ever wondered why? The answer is simple – our data. This data set is collected on the basis of our likes, comments, posts we share, things we may read, the videos we watch etc. This data is later used to influence your choices ideas and everything that you may do in your daily lives.

Data

1. Data are characteristics or information about you

2. Data is stored in such a way that it can be processed.

3. Data can be used to influence you and to monitor your activities, behaviour, and practices.

4. All interactions with the Internet can be collected, stored, and processed as data.

5. Businesses, governments, and many other organisations use data to improve their work efficiency.

Is data collected only by social media platforms?

No. All businesses and government entities collect data about customers and citizens in one form or another. Businesses and who provide digital services are able to capture very granular data on basis of mobiles applications that are provided by them to the customer. However, the practice of enumeration and data collection stretches back to colonial times. Data of the number of households in India was first collected by the British in 1872.

Since then, governments have collected data like census data to enable better administration and policy planning. However, data aggregation by government today have also come to include digital identification systems like Aadhar Card which contains digital biometric information. This is in turn linked to a large extent to other utility services we use like banking, mobile phones etc.

The stated aim of the Aadhar project is provide seamless social protection delivery to eligible populations without leakages. The data triangulated across the social protection database provide a 360 degree overview of an individual.

Is data collected only by social media platforms?

1. There have been various data collection practices at various points of time.

2. Census is also a way of collecting data.

3. The government uses data to formulate policies.

4. Data aggregation by government has come to include digital identification systems like Aadhar.

5. The Aadhar data triangulated through linkage with utility and social protection services provides a 360 degree overview of an individual.

Different Ways to Collect Data

2021
Census

Applications

Website

Social Media

Google

Aadhar Card, Health Card etc

Do private entities also collect data?

Yes. Private firms, financial institutions, digital payment systems also collect vast amounts of data. From Ola, Uber to Paytm and Zomato, every application that we use on smartphones or computers collect our data and process it.

There are two types of data:

1. Personal data:

Any information that relates to any individual, or different pieces of information which can lead to the identification of a person is called personal data. Personal data constitutes a mobile number, name, birth certificate, etc.
Personal data can also fall into the category of sensitive personal data which are those aspects of personal data that need extra security like you religion or caste, political opinion, mental health etc

2. Non-personal data:

Any anonymous data or data which cannot lead to the identification of an individual is non-personal data.
Non-personal data includes data of climate collected through the weather apps.
Cab apps such as Ola, Uber and, social media platforms such as Facebook, Instagram etc. gather both personal and non-personal data.

Do private entities also collect data?

1. You can be directly identified by your personal data.

2. You cannot be directly identified by your non-personal data.

3. Personal data can also be classified into sensitive personal data which require extra security.

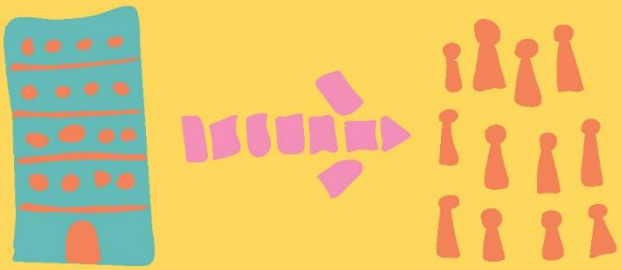
4. Non-personal data represents computer patterns, climate data, traffic patterns. Non-personal data are not tightly regulated.

5. Social media platforms collect both types of data from different applications that you use.

Why is data so important?

Data can be used for different purposes depending upon who is collecting the data. Big firms use the data to improve their efficiency. Data helps in organizational decision making, and to steer the future strategies. Data helps the organization to visualize the relationship between what is happening different locations. The government can potentially use the data in an attempt to bring equality in society by formulating policies and ensuring fair representation of everyone.

1. Data can be used to predict your behavior.



2. From insurance companies to chocolate companies, every company is using the data to target, identify, and sort their customers.

3. The data is used by the government to determine everyone's stake in the policies.

4. Data is also used to improve traffic, law and order etc.

5. But, the usage of the data can be discriminatory as well.

So what's the problem?

Data can be used for good as well as bad purposes.

Previously, we saw how data can potentially be used as a force for good. However, data is a powerful tool which gives immense power to those who have control over it. Data security has increasingly become a cause of concern. Security of Aadhar data has increasingly been called into question by public interest technologists while the government has denied any breach. Further, your social media data can used to influence electoral outcomes.

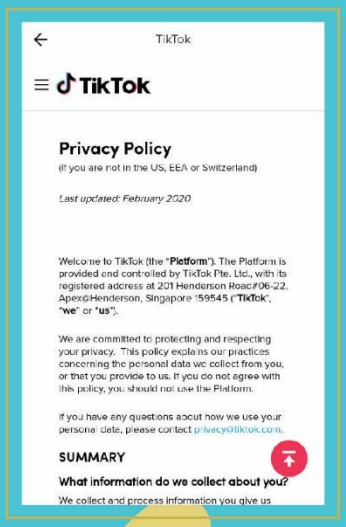
The Cambridge Analytica scandal showed how data of up to 87 million Facebook users were used to influence voting patterns and electoral outcomes. Cambridge Analytica has worked for the 2016 Trump Presidential Campaign. Moreover, financial institution have come to use individual's social media practices as proxy for creating risk profiles and determining creditworthiness.

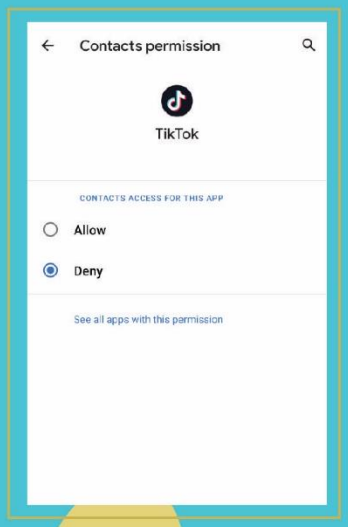
An electoral analyst can predict voting patterns as per issues, demographics, and behaviour. How worried are you about national security? What do you think about the economy? What do you think about law and order? You are likely to vote according to the issues that affect you. And you can be persuaded through social media to vote according to your likes and dislikes. This creates filter-bubbles and close out democratic spaces for discussion. This undermines a citizen's rights in a democratic system.

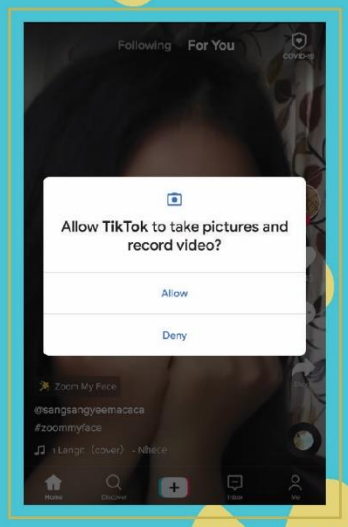
Political parties, along with corporates, will continue to appropriate social media to influence the voter during election time. The imbalance of power exerted by powerful stakeholders have a pervasive impact on constraining citizen's democratic rights.

Sois the information being collected with our consent?

Have you ever noticed that when you download an application on your smartphone, a big essay pop up your screen and you are asked to tick a small box? When you tick this, the app takes consent from you about the information can be accessed from your smartphone and how and where such will be used and with whom it will be shared.







Consent means that you are agreeing to do something, or you allowing someone to access your information. If someone comes to your house to ask for health, education, or any information, then you can ask them why they are asking for these pieces of information. In the same way, you also have the right to give consent on the internet, too.

So the information is being collected with our consent?

1. The danger of misuse of data is becoming more critical than ever.

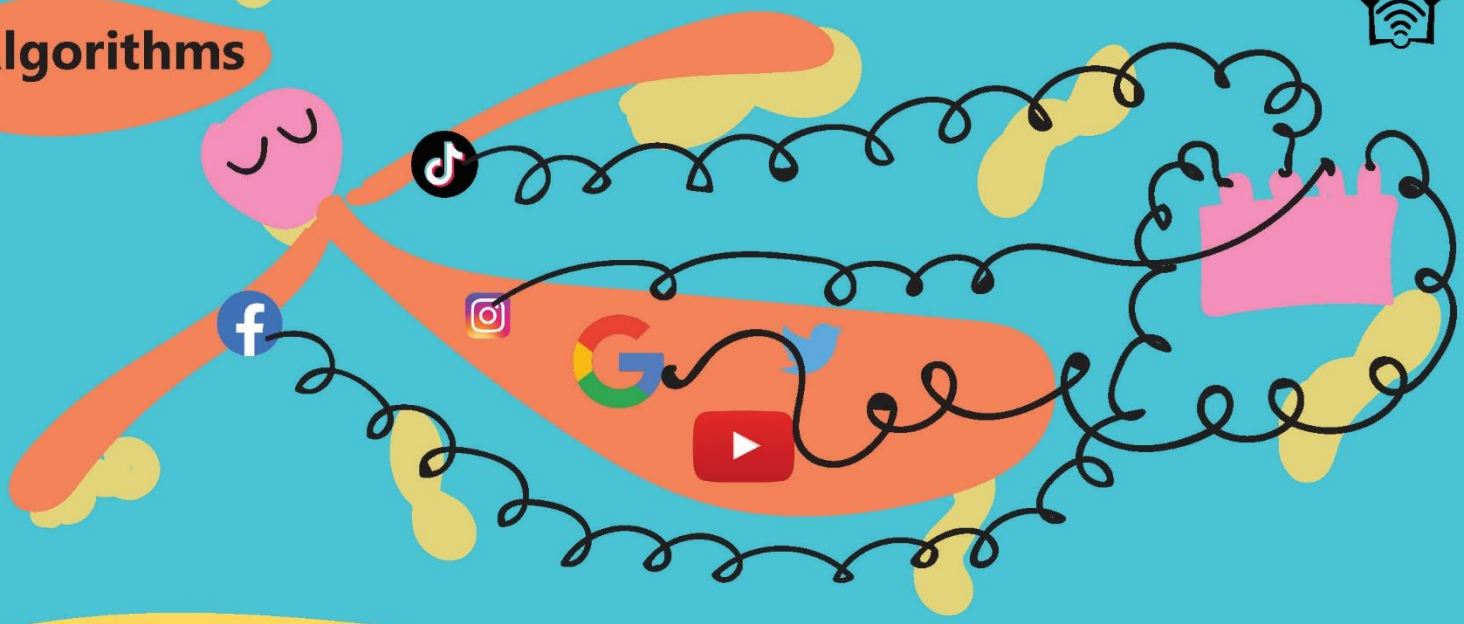
2. Data security remains a pertinent issue.

3. Personal and non-personal data can be used to influence voters.

4. Transparency on the use of data is crucial.

5. With artificial intelligence gaining ground data will come to play even more structuring role in the future.

Algorithms



An algorithm is a technique that anticipates user behaviour and/ or completes a given task on their behalf. It is a process of self-learning by a computing system of processes that it is used to automate or predict. It uses data to learn, the more people use a system, the more it learns from their behavior and the better its predictive ability gets. Based on a person's usage patterns, social media platforms always try to give preference to the content which the user might want to see first.

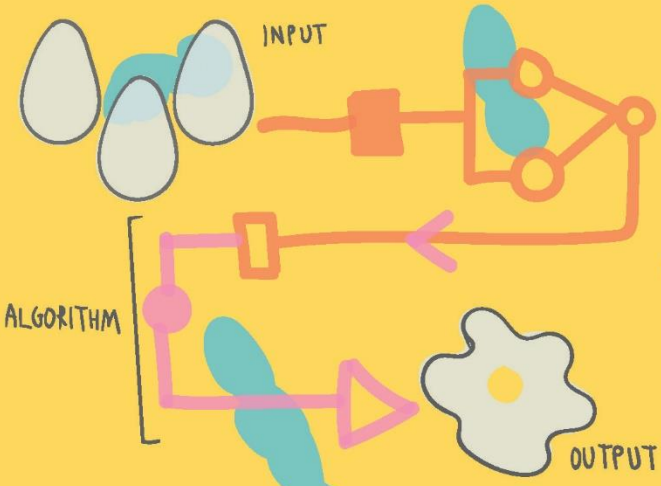
Have you noticed that when you like a page, then the same type of pages start coming in the suggestion box? If you watched a video, more videos of similar type start popping up. Whatever you like, watch, or shop – similar content or product will be pushed towards you. If you try to search on national security, then you will begin to see content related to national security everywhere from YouTube to Facebook. And with this kind of filter bubble, it's challenging to develop an unbiased opinion on any issue.

The algorithm creates an imaginary world around you. On the Internet, everyone is living in a virtual world, according to their belief system. Filter bubbles has made it easy to polarise society, to spread fake news, and to peddle rumors.

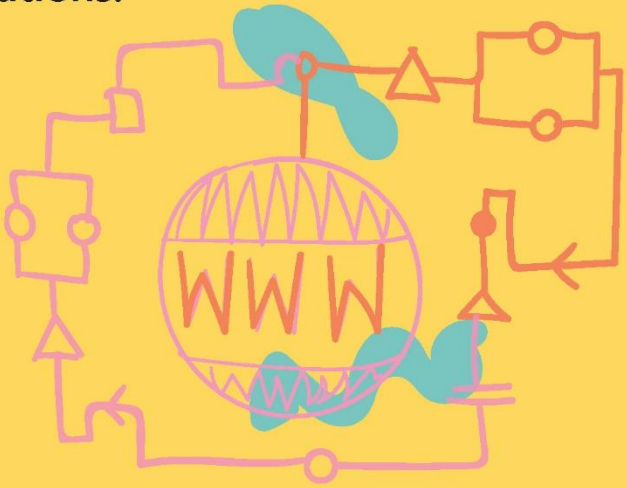
All of the above is operationalised based on your information using data driven techniques. Every application knows something about you. Your mobile alarm knows when you wake up. Your Google Map knows which route you take to reach home. Your Google Assistant knows when you are angry. Swiggy and Zomato know when and what you love to eat.

Algorithm

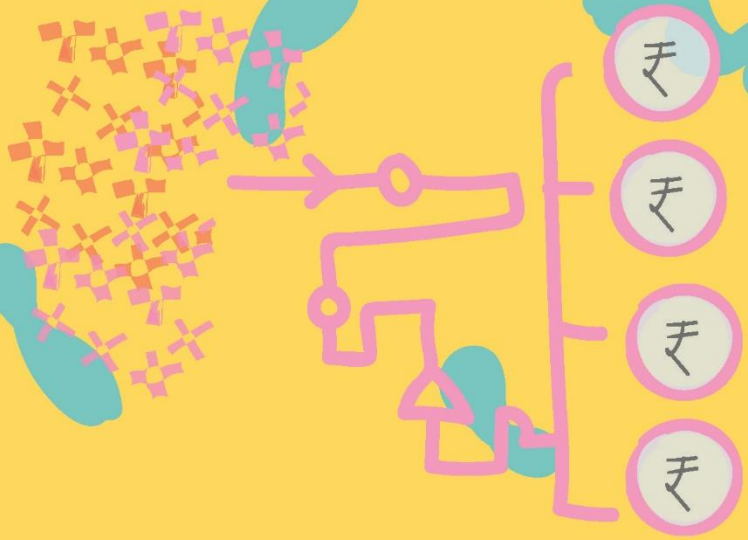
1. The algorithm tries to show you the content based on interest rather than relevance or accuracy.



2. The purpose of the algorithm is to optimize everything which also raises ethical concerns in morally complex situations.



3. Complex algorithms are increasingly being deployed on large and complex data systems and structures extracted through the provision of digital services



4. Data driven techniques sort, analyze, and predict with the aim to optimizing business objectives

5. Filter bubbles created by algorithms have made it easy to polarise society, to spread fake news, and to peddle rumors.

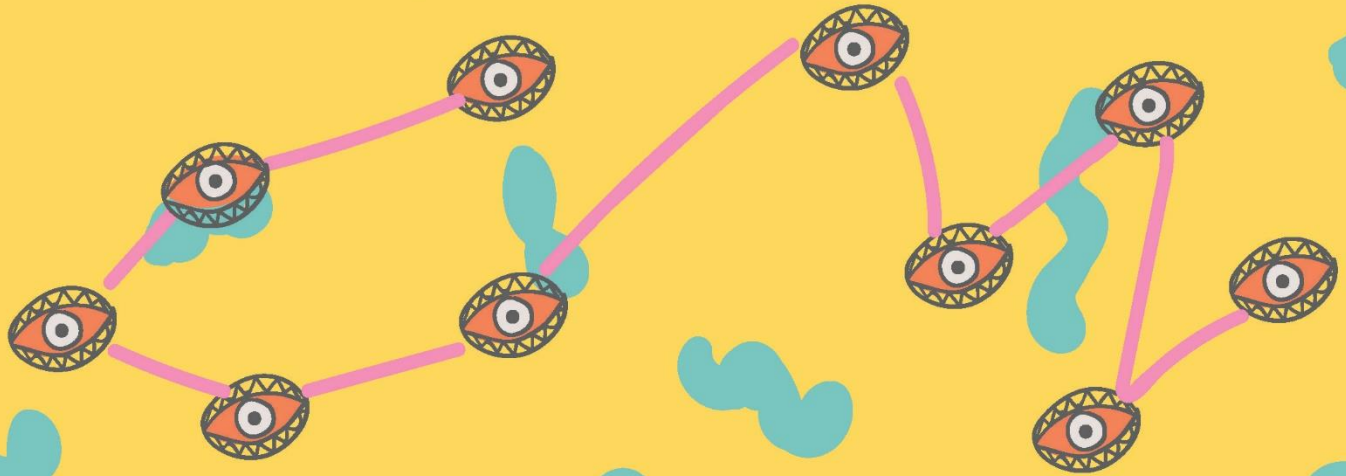
Surveillance

Public places like railway stations, cinema halls, and now even workplaces are being monitored through CCTV (Closed-Circuit Television) camera. Have you ever thought that who is keeping these data that is being gathered? How safe is the information?

Governments have highlighted how CCTV cameras have helped to thwart crime. My state government are using CCTV cameras along with legacy data and sophisticated predictive policing algorithms as a law enforcement measure. News reports mentioned the use of facial recognition systems deployed during December 2019 protests. This led to questions of privacy and discrimination given the documented instances of such softwares to be discriminatory against minorities and marginalized communities – thereby leading to the tagging of such communities as inherently criminal. Many governments around the world are deliberating the banning of facial recognition softwares in policing as a result of their discriminatory potential.

For example, if the machine learning and algorithms show that there is a higher probability of crime in a low-income neighborhood then its increases the likelihood of people in that particular neighbourhood to be classified as criminals.

This would result in false positives and criminal profiling as per social and economic status creating greater possibility of discrimination, harassment and exclusion for those communities and the children who grow up there. In the garb of lowering violence there is increase in surveillance activity. Then the question is, do I have any privacy? Or am I being watched every single moment? And how am I being classified?



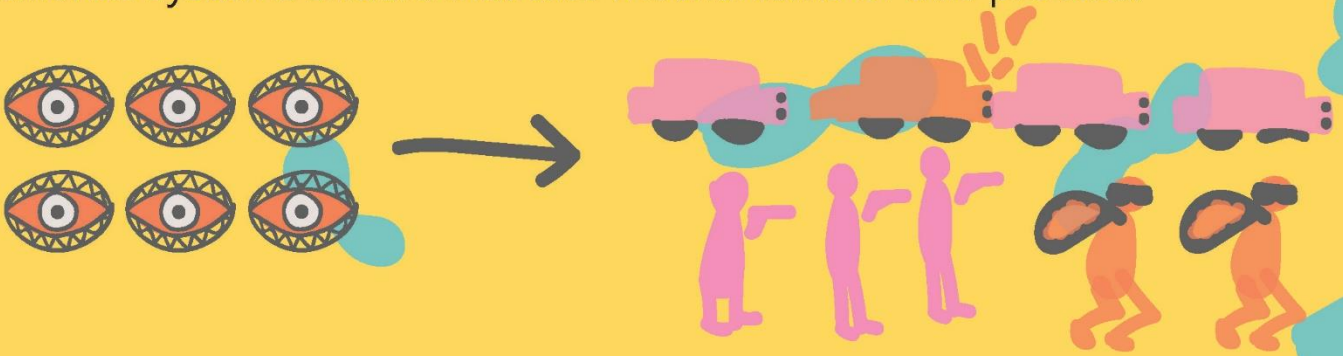
Surveillance

1. Surveillance without transparency can sort and classify on indicators that would lead to exclusion and disenfranchisement.

2. The accountability should be fixed, who and why are we being watched and on what basis such decisions are taken.

3. Over surveillance can lead to a more severe form of censorship which will distort the flow of information.

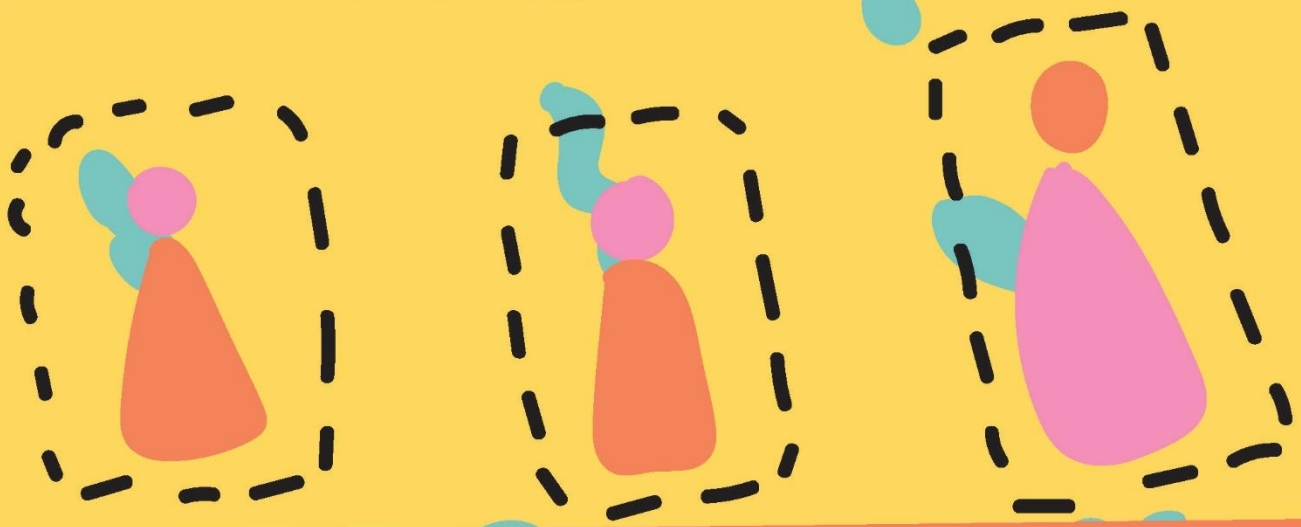
4. Surveillance systems should institute mechanisms of due process.



5. The question of monitoring should be seen in the context of necessity and proportionality without infringing on the right to privacy.

So what is privacy?

Remember the days when we used to get phone calls or messages, every single day, to link the bank account with an Aadhaar Card. Have you ever wondered why we don't get them now? The Supreme Court of India, in its historic judgment, recognised privacy as a fundamental right.



The Supreme Court said that the Right to Privacy is a fundamental right protected under Part III of the Indian Constitution. It is an intrinsic part of right to life and personal liberty under Article 21 of the Indian Constitution.

Privacy is contextual. The boundaries of what is considered private vary between cultures, society, and individuals. Your idea of privacy and its limits may be different in your homes and in online spaces. Further, towards the exchange of your information online, your expectations of privacy might be completely different.

So what is privacy?

1. What would be your reaction if someone starts keeping an eye on everything all the time, What do you do, what you eat, what medicines you take, where you go, what you think, what you watch online?

2. Privacy is a fundamental right, guaranteed by the Constitution of India

3. Every individual has every right to keep anything private, until and unless it is not a criminal offensive.

4. If our privacy gets affected, our ideas, thoughts everything would be affected due to the fear of being watched every time – leading to what is called the chilling effect – people too afraid to express themselves.

5. Democracy will be in real danger if our personal details like political party we support, idea of the political spectrum we like etc., are kept under close vigilance.

So what next?

Technology is no longer limited to making instruments and machines, it is furthering techniques which are more potent and powerful than ever before. Artificial Intelligence (AI) refers to the simulation of human intelligence in machines. They are made to think like humans and imitate their actions and speed up actions that would take an individual a lot of time to get done.

Resources can be saved using Artificial Intelligence. It can be used to regulate traffic, to improve agricultural productivity, save lives through preventive screening in healthcare etc. It can prevent suicide, violence, and almost everything, which only a few years ago seemed impossible for a machine.

However, without the data, AI is nothing but a toy. All these fascinating developments would not be possible without the data; as mentioned earlier, AI is an entirely data-driven technology. And, despite all these great developments, pertinent challenges of AI have not been addressed.

In the data-hungry world of the future, which is just a moment away, we would increasingly be classified on the basis of the data gathered about us from different sources. So there needs to be greater transparency and safeguards in place for us so that we know how our data is collected, how it is going to be used, and what rights we have pertaining to that data.

So what next?

1. Greater use of AI would lead increased classification of people on the basis of data collected about them.

2. We should know how our data is collected, how it is going to be used, and what rights we have pertaining to that data.

3. AI would collect data from multiple sources in whichever sector or function it is deployed in

4. AI is a uniquely data-driven technology.

5. AI has a humongous potential to bring positive changes, but the danger of it being wrongly used remains a menacing challenge too.

Why should I worry about Artificial Intelligence?

Discrimination

From governments to private firms everyone gathers information about us. They determine what ads we would see. Based on these data sets, Governments formulate policies. These policies affect us in many possible ways. Imagine, if criteria for the job or loan and, the eligibility of the scheme is done based on these data sets through not very transparent techniques – like using your social media activity to build risk profiles determine credit-worthiness or as a proxy for stability in a particular job – how would you feel?

Decisions based on these data and the use of AI can reinforce inequalities and discrimination that already exists in society. This discrimination is likely to affect the vulnerable sections of the society most – remember the example of criminal risk profiling mentioned above. Those who will not be able to fall within some predetermined matrix with built-in classifiers will be overlooked by the Governments too. The discrimination will be clinical.

Why should I worry about Artificial Intelligence?

Transparency:

Despite all the enthusiasm about the success and developments of AI, many critical challenges remain unaddressed. As algorithms become more advanced, understanding their internal functioning has become ever more challenging. One of many reasons is that the companies developing them do not allow independent examination of their algorithms, rather they are trying to convince that AI is becoming vague due to its increasingly complex techniques. With AI becoming even more pervasive in our day to day lives, if efforts are not taken to make its process more transparent and inclusive, it will have a devastating effect on the most marginalized sections of society.

Why should I worry about Artificial Intelligence?

1. How would you react if every important decision of yours, like whether you will get a loan or not, you will get admission to a college or not, you will get a job or not, are all based on the datasets and machine learning with opaque processes?

2. Transparency in decision-making of AI systems is a major concern.

3. Without a transparent system, AI may exacerbate discrimination.

4. In the era of AI, securing the privacy of an individual would be a major challenge. Techniques like facial recognition could be a tool for harassment.

5. The chances of exploitation of your emotion, ideas, and beliefs would increase.

So what is the Government doing?

The Government of India presented the Personal Data Protection Bill to regulate the data. The bill is currently being analyzed by the Joint Parliament Committee. The Government has proposed that the bill will protect the personal data of every Indian and its usage will be categorically specified. The bill also addresses the issue of cross border data transfer and accountability of entities. But it gives a huge exemption to government institutions and agencies with very little due process.

The bill will also provide tremendous power to the government to access citizens' data any time. The bill was heavily criticized for ignoring the privacy of the citizens. Less autonomous power has been given to the Data Protection Authority. Over centralization of information would create an atmosphere of fear, distrust, and democratic rights will be eroded.

So what is the solution?

1. A strong law would ensure protection of personal data.

2. The law should ensure transparency.

3. The accountability of the entity, who processes the data must be fixed.

4. Privacy, which is a fundamental right, must be respected.

5. The legislation must include due processes for Government entities as well.

So how can you ensure safety of data at the moment?

Social media platforms are places where you spend a lot of time doing numerous activities – right from chatting to posting your views to uploading your photos, everything. So it is important to manage privacy settings on your phone, laptop, and every social media platform that you use.
Almost every application asks information about you like, where you live, which school you have attended, what interests you, where are you currently working, where did you work before, or which political party or ideology do you support.

Many applications ask for more personal information. All these pieces of information may seem harmless at first glance, but it can be stored, processed, and tracked. It can be used by big firms to sell their products, and political parties may use it to influence you.

So in the times of emerging new techniques and smartphones, we must be cautious about the privacy settings of these applications. Here are some suggestions that you may find useful.

So how can you ensure safety of data at the moment?

1. We understand that reading the terms and conditions of these applications is a tiresome task, but try to read it.

2. Be cautious about the information being asked to share.

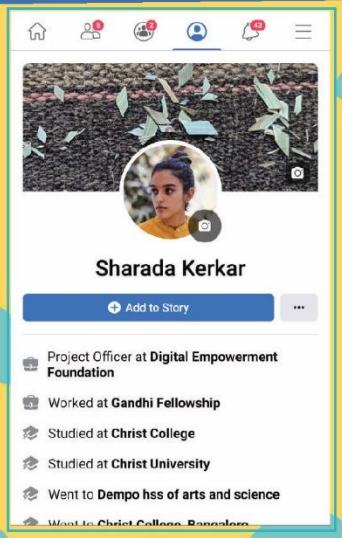
3. Try to avoid sharing your personal information as much as you can.

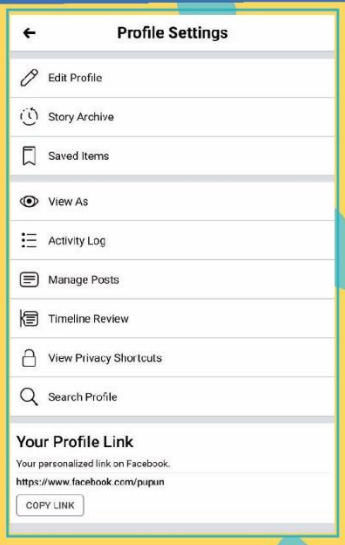
4. Share photos, videos, any information, or any news on social media with high discretion.

5. Keep an eye on your phone's privacy settings as well.

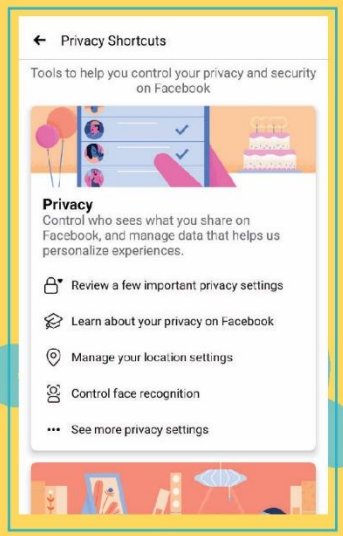
Facebook

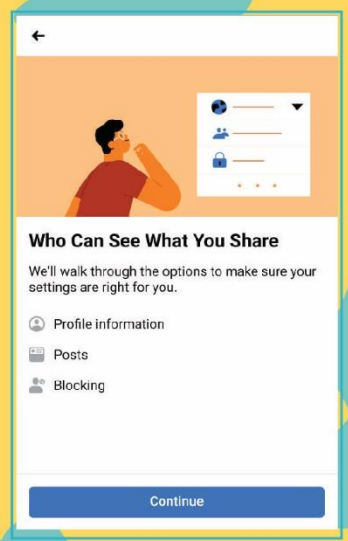
1.First, choose who can access your information. You cannot hide some information like name, profile photo, etc., but some information can be managed like your activity, your post, your friend's list, etc. To make a change, click on the three-point option on the right-hand side of the Facebook profile, and manage your activities and privacy settings.



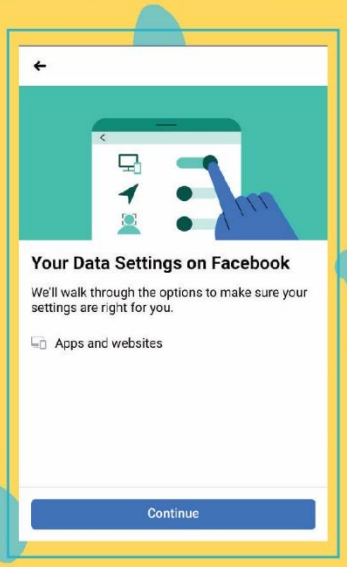


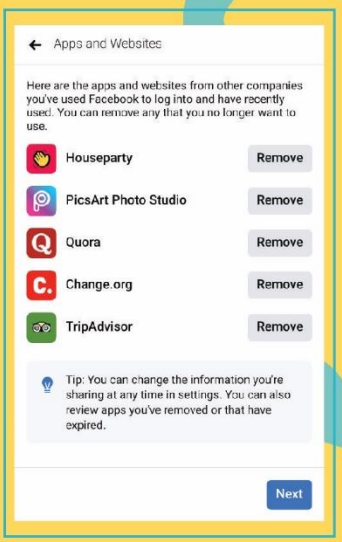
2. Be cautious about the posts you share with. Before posting anything, there is an option in the top right, in which Facebook asks you to choose with whom you want to share-only to yourself, to your friends, or to the public means anyone. Choose 'your friends' option.



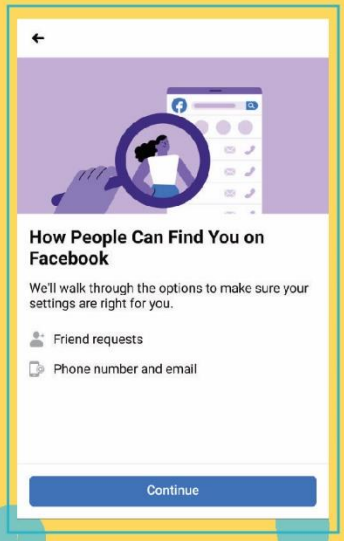


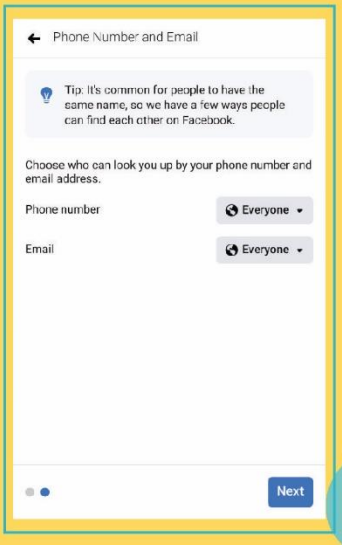
3. Don't grant any third-party applications to access your Facebook profile. When you download a new application, you might be asked to log in through Facebook in order to sign you up for that application quickly. Such applications can keep track of the activity of yours on Facebook. You can disallow those apps by clicking on Data settings > Apps and Websites.



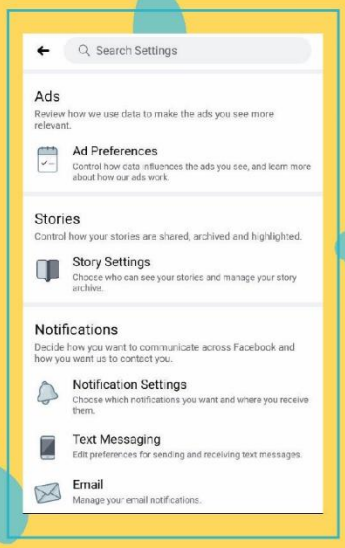


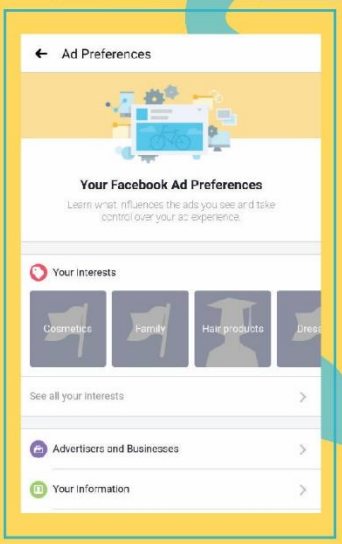
4. You can prevent your profile from appearing in Google search by disabling in the privacy setting.



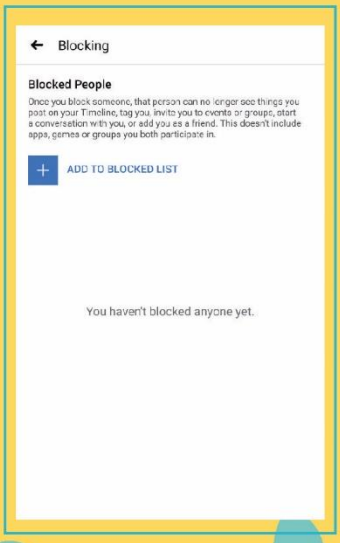


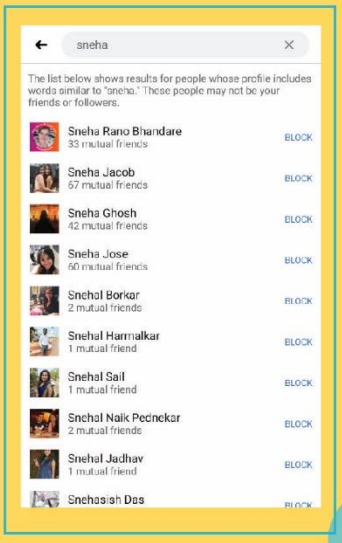
5. Facebook keeps tracking your browsing activity everywhere and uses these data to provide you with more personalized advertising. You can manage it too. In the Menu Settings, on the left click on "Advertisement". In the first section, Facebook will display your interests. If you turn this setting off then you will still be able to see the same number of ads but these will not be based on your web history.





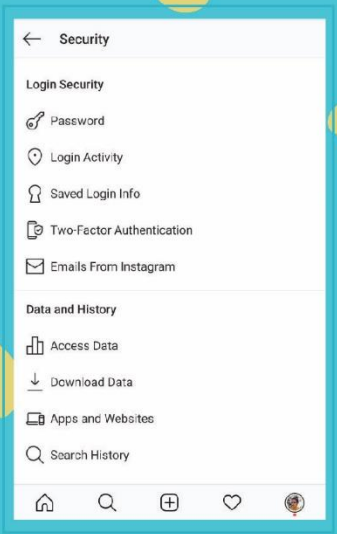
6. Immediately block suspicious users.

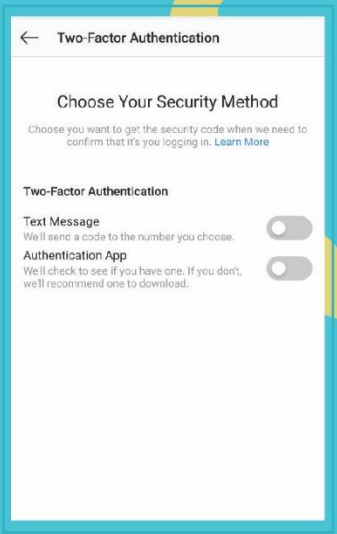




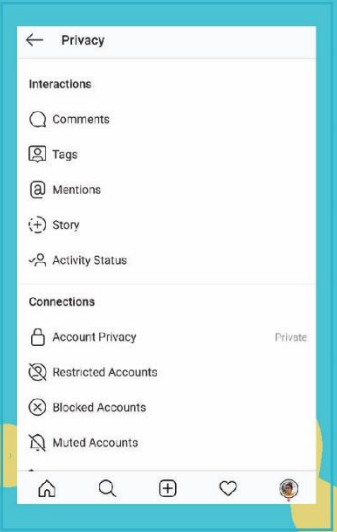
Instagram

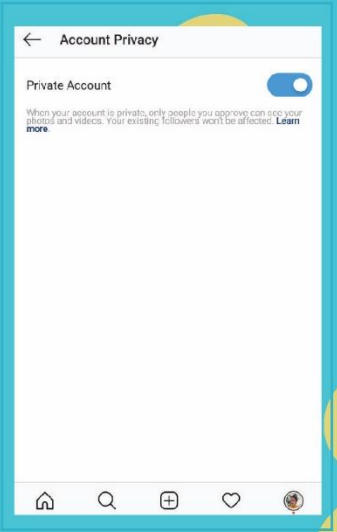
1. To keep your account more secure - go to Profile > Settings > Security Option > turn on Two-Factor Authentication > turn on text message option too.



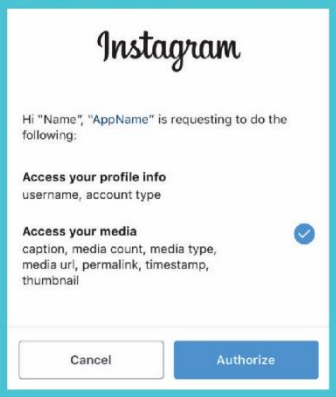


2. To keep your account private, click on the profile to make it private, go to Settings > Privacy > turn on 'Private Account.'

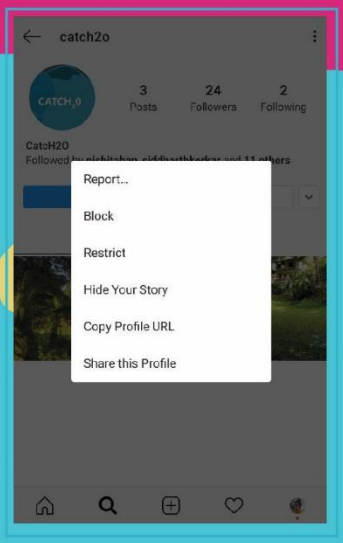




3. If a third party application asks for your permission from Instagram then, allow it carefully. Review what information it is asking for. You can also remove it. Go to Settings > Authorized App > manage your settings.

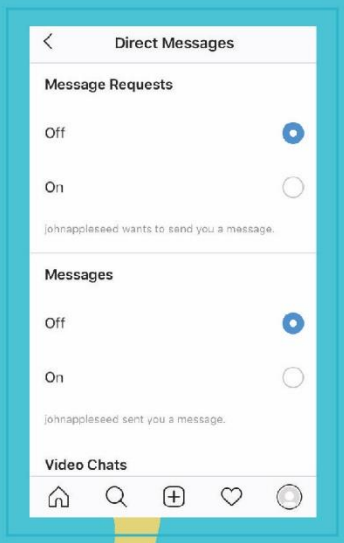


4. Block the suspicious user immediately. To block someone, go to their profile, and click on the three-point option, and the block option will pop up on your screen.



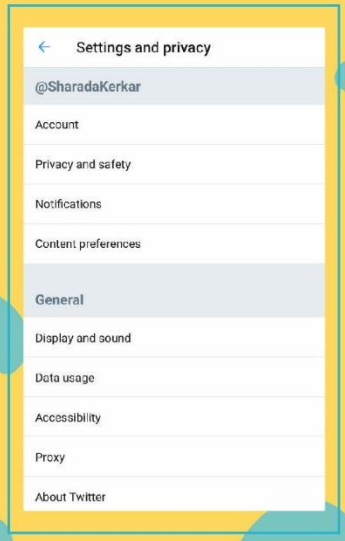
5. You can turn off the active status on Instagram. Go to Settings > Active status and turn it off.

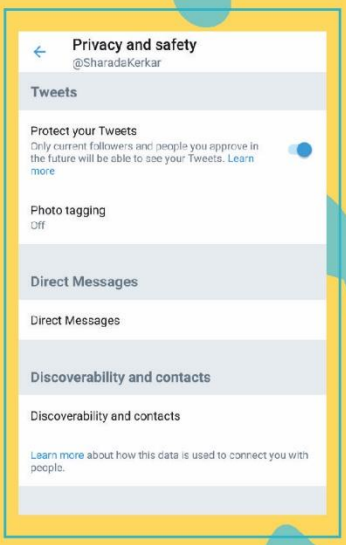
6. You can turn off the direct messaging facility. To do this, go to Profile > Settings and turn off the direct message.



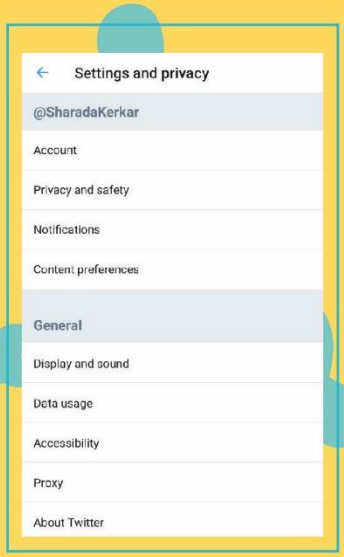
Twitter

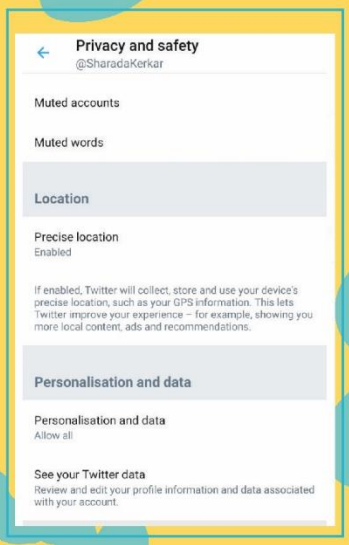
1. You can your account private. To do this, click on the Profile > Settings > Privacy > enable 'Protect Tweet'. At the same time, an option will be shown below, the tweet location meaning that the place you have tweeted from, from which phone, etc. – you can turn it off.





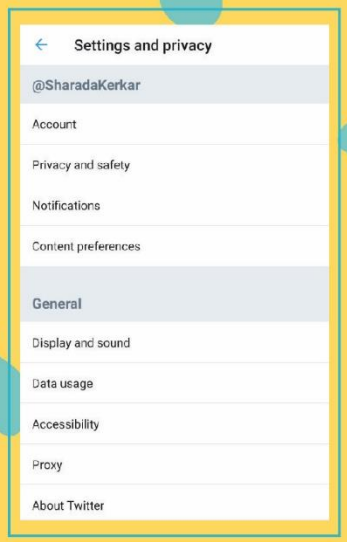
2. Within security settings, Twitter allows you to manage how much information Twitter will use. For example, most options are fairly self-explanatory - personal ads or sharing the data with Twitter's business partners etc.

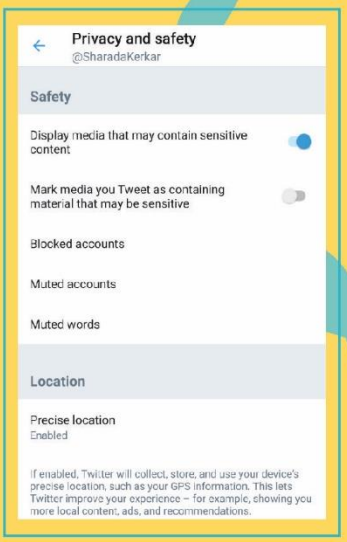




If you have enabled the 'Personalize based on your devices', Twitter might pick up your data from different platforms to show you more personalized advertisements.

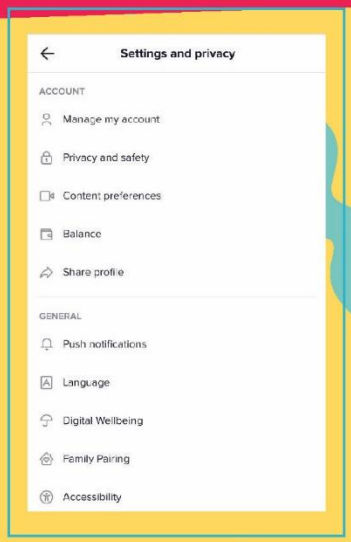
3. By going to settings, you can also decide whether you are interested in seeing sensitive posts or not. You can turn it off and also block any suspicious user.

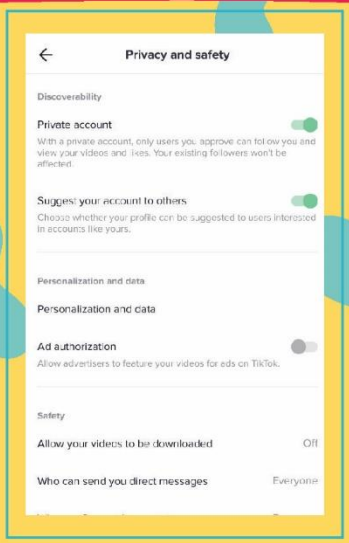




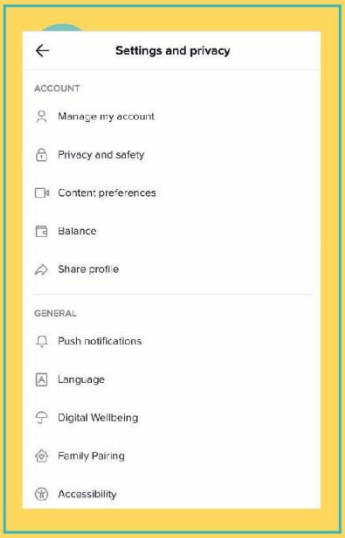
TikTok

1. You can keep your account private – in order to do that go to profile, click on the three-point option on the top, click on the option of privacy and settings, and make it a private account.

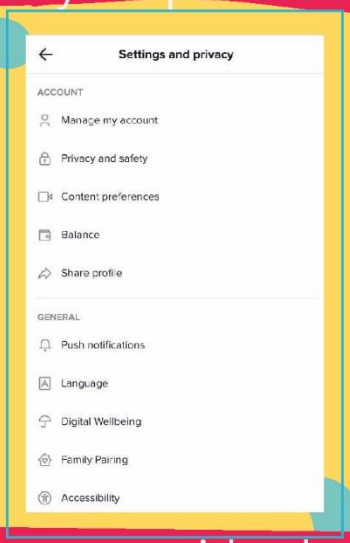




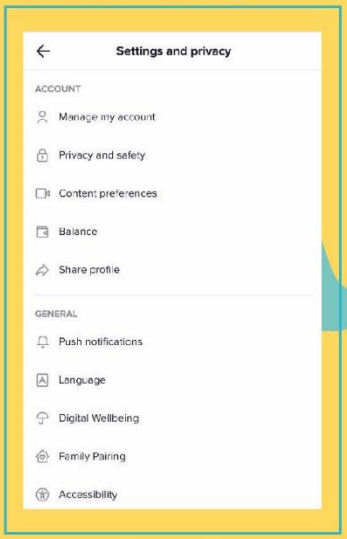
2. By turning of digital well-being, you can decide the time a child can use the app and ensure that inappropriate content will not be shown etc. In order to do this, go to the settings of the TikTok App and turn on digital well-being. You can also add passwords to make it more secure.

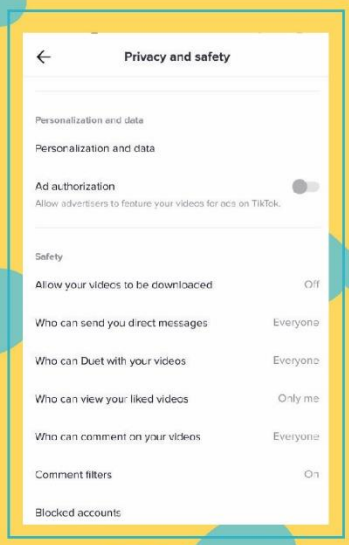


3. If you want to control your comments, go to Settings > Privacy and Safety Settings > 'Who can send me a comment' and choose your option as per your preference.

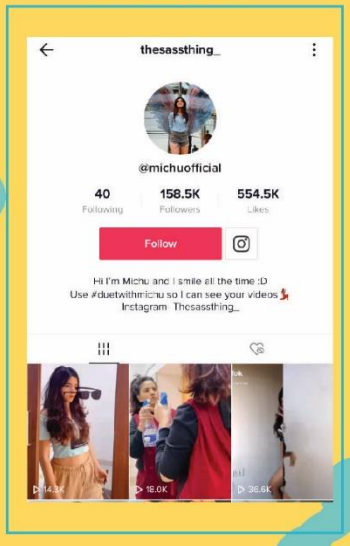


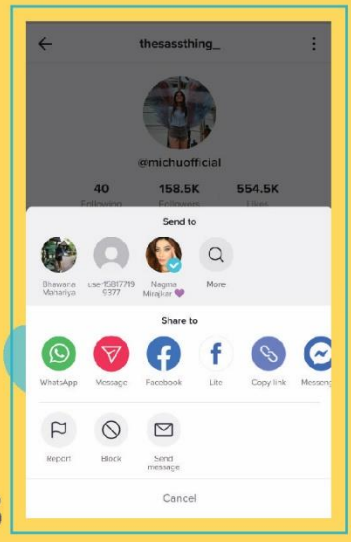
4. You can also manage with whom you wish to do duets. Click on the privacy and safety setting > Tap on 'who can duet with me' and choose the most suitable option.





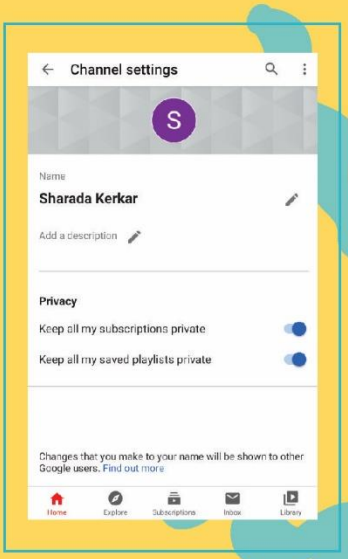
5. Block suspicious users immediately. To block someone - go to their profile, you will see the block option when you tap on the three-point option.

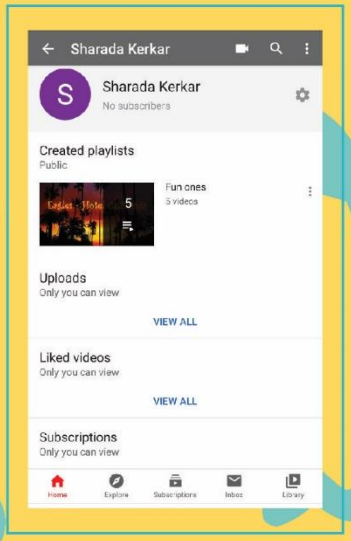




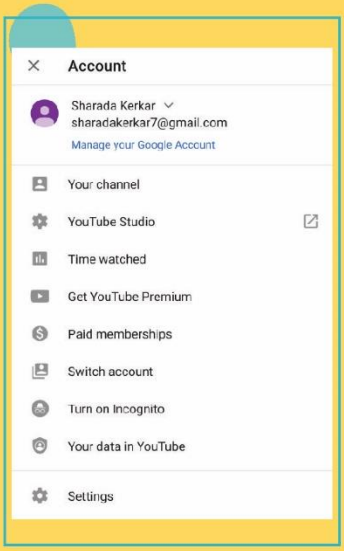
Youtube

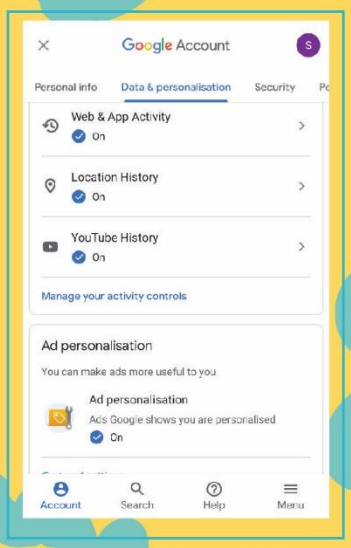
1.What you watch and what you like can be kept private. In order to do this go to Settings > Privacy. Now, many options will pop up on your screen like videos that you have liked, you have saved, and the channels you have subscribed to – you can tick the options as per your choice.





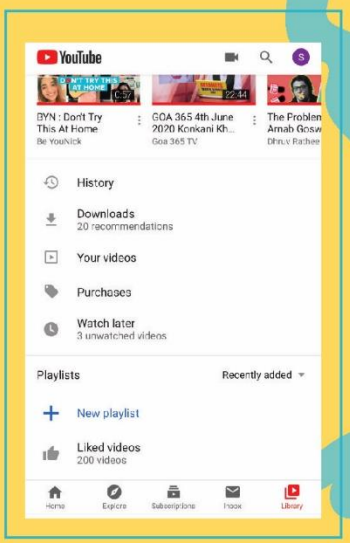
2. Google keeps an eye on YouTube videos that you watch and uses this information to show you personalized ads. But if you don't like it, you can turn it off.

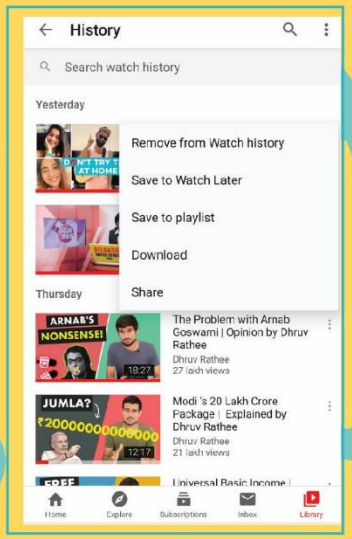




If you don't mind personalized ads, but still want some control over your privacy, you can remove some information about your interests. For example - your interest in music. Go to the privacy settings of your account, there you will see the option of 'Ads based on my interest' you can change your preferences there easily.

3. You might want to keep deleting the watched videos frequently, in order to do this click on the library on the right side of YouTube, the history option will appear when you can click on the three-point option beside any video and delete that video.

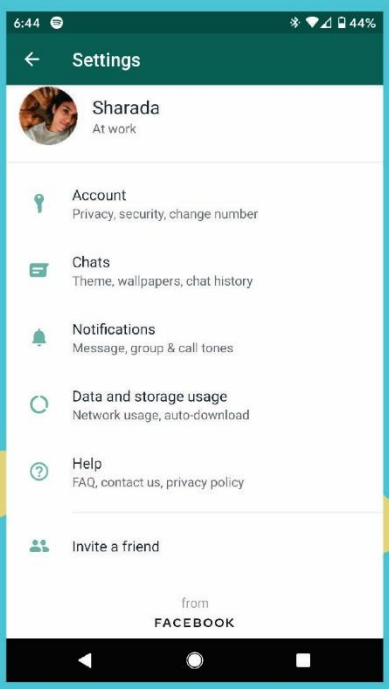


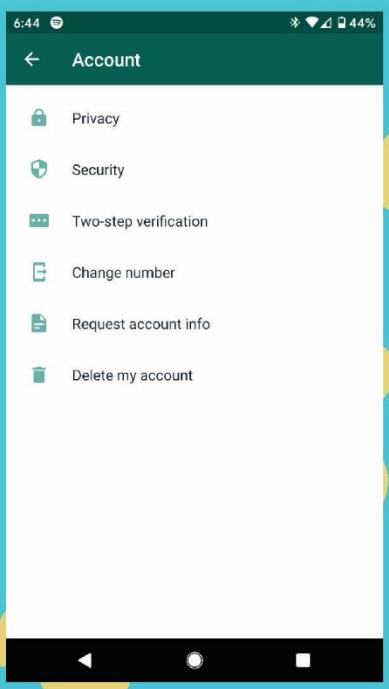


WhatsApp

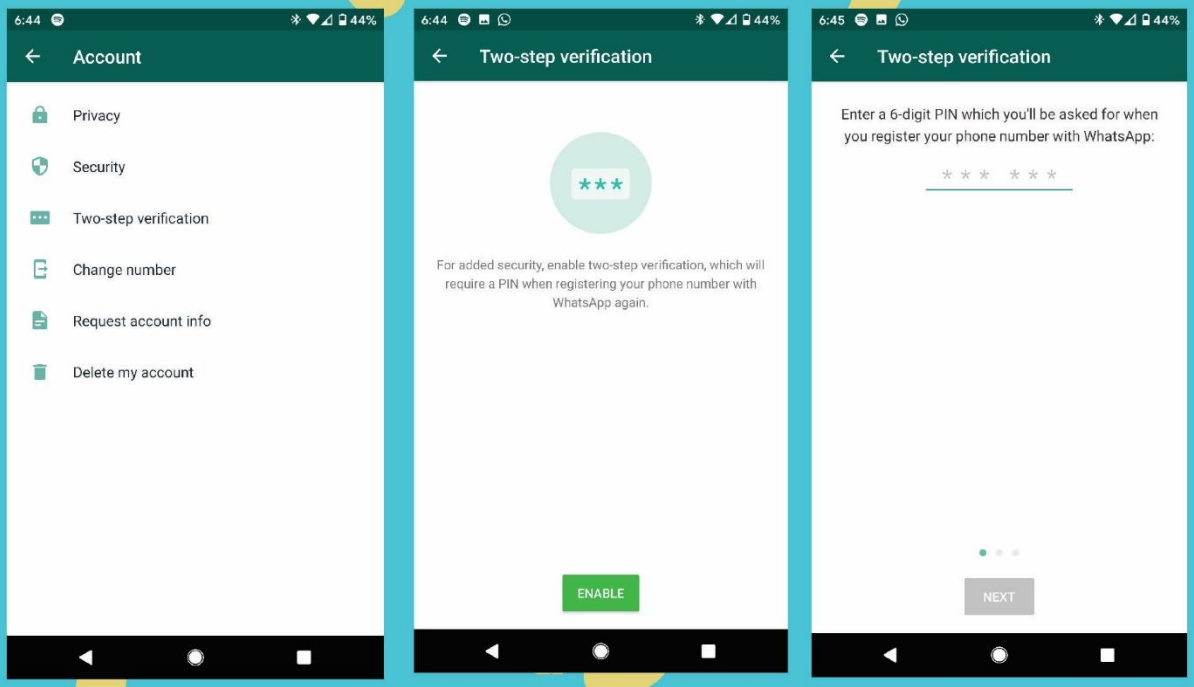
WhatsApp is one of the fastest-growing instant messaging services, and it has changed our experience of communication completely. WhatsApp, however, works on an end-to-end encryption technique. It is the default mode of WhatsApp and cannot be turned off. Encryption ensures that your messages can only be read by the recipient. Similarly voice and video calls too are encrypted. At a time when everyone is struggling to secure privacy, encryption provides much-needed privacy for the online activities. Here are some small steps which you may take to enhance your security and privacy on WhatsApp.

1. Each conversation on Whatsapp is encrypted with unique QR code and 6 digit numbers. You can verify these codes. And, when the security code is changed, WhatsApp can send a notification. Go to the settings option of WhatsApp, click on the account, and go to security and turn it on.



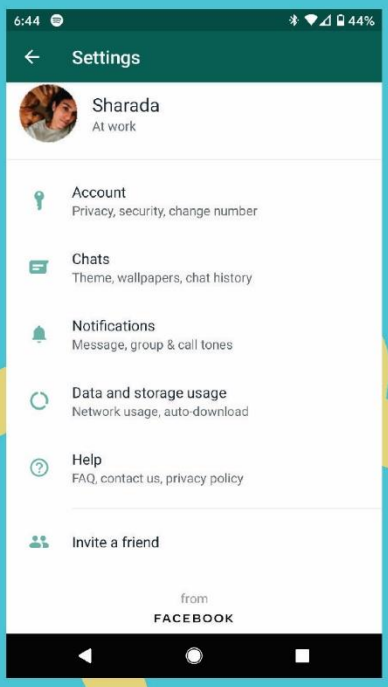


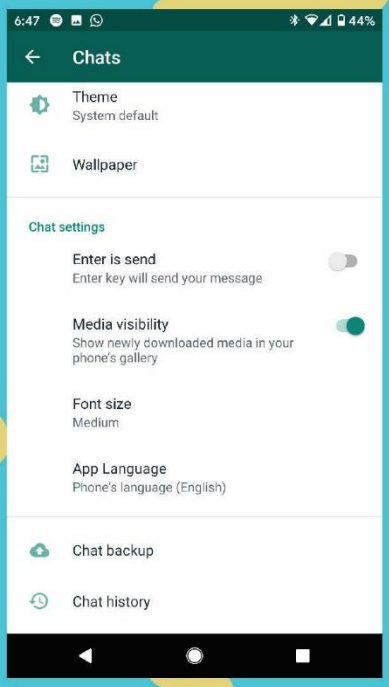
2. Turn on two-step verification. This will make your data more protected. To activate two step verification- go to the Menu > Settings > Account > enable Two-Step Verification. Create a six-digit PIN code that you can remember easily. If you forget it, add your email address to retrieve that code.

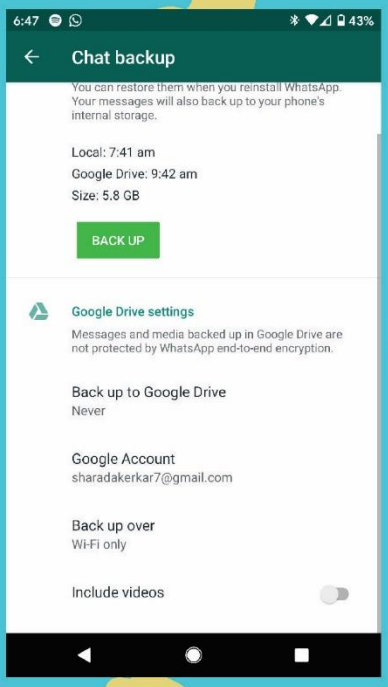


3. Do not click on any kind of suspicious link. This will increase the risk of your chat being hacked or data being robbed.

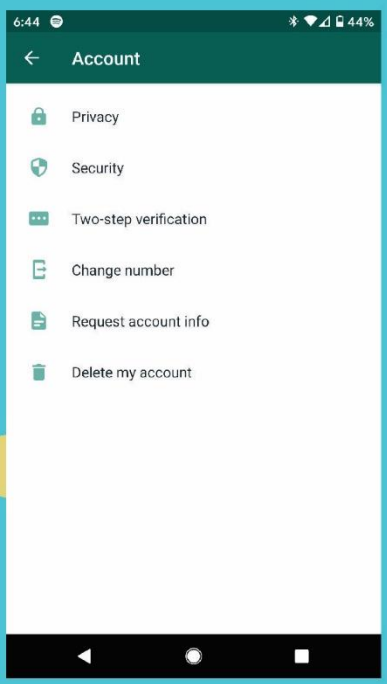
3. You can opt-out out of back-up on Cloud: Data saved on the cloud - like Google Drive, or iCloud, etc. makes tracking easier. To turn it off- go to the menu, tap on settings, open chat, go to chat backup and click on 'never'.

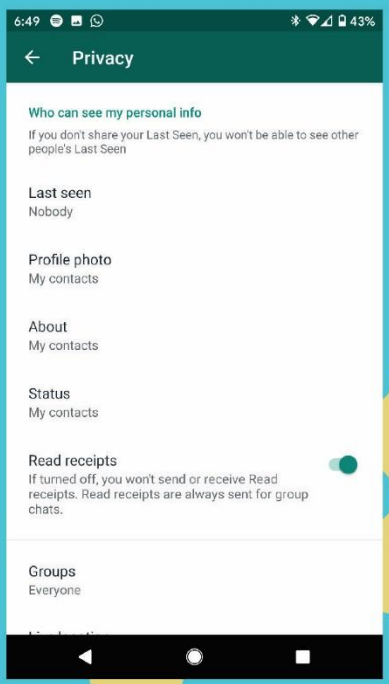




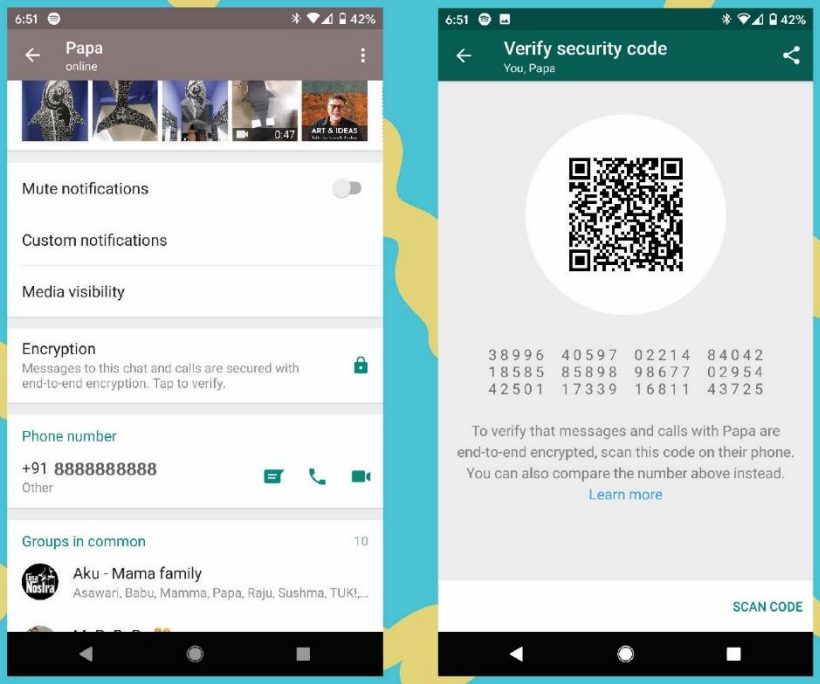


5. WhatsApp is not the most private messaging app, but it gives users at least some control. You can manage your preferences. Go to settings, click on the account, and go to privacy. You can control who can see your last seen, profile photo, status, and live location, choose the option as per your choice. You can also hide the read recipients, it turns off the blue check-mark.





6. Even though WhatsApp claims to encrypt all chats by default, sometimes it is better to double-check, especially when you are sharing sensitive information. To verify encryption, in that contact's chat window, tap the contact's name, and then tap encryption. You will see the encryption code. It can be scanned and verified.



What if I use laptop/computers too?

If you use a laptop or computer, you can use the Firefox browser, it is more guarded. Click on the privacy settings in the browser, you will get an option - "Tracking protection in private windows"- you can make it default.

Data Rights for Communities is resource document created to generate awareness about changing nature of rights in a rapidly evolving digital world. With data becoming an integral part of our lives it is crucial that we understand how our data it is being used. Data is being used in transformational ways that can be used to bring about progress and prosperity. However, given the power and control that comes with ownership and processing of data has led to grave concerns about the threats of its adverse usage. Therefore, it becomes critical that we understand its impact as well as the rights associated with it.

DEF
DIGITAL EMPOWERMENT foundation
Digital Empowerment Foundation
www.defindia.org