JUSTICE adda

THE (NOT SO) SECRET LIFE OF YOUR DATA

JUSTICE adda

CONTENTS

JUSTICE adda

HOW DATA WOKE ARE YOU?

MODULE 1

HOW DATA WOKE ARE YOU?

Take a quick self assessment to find out how aware you are of the usages and implications of your data. There is an answer key at the end which will help you.

1 What do you think personal data is?

A. Your name, Instagram handle and home address- nothing else

B. Passport details, Aadhaar card, insurance and bank details

C. All of the above- personal data is information that can be directly or indirectly used to identify individuals

2 How much do you think big tech companies know about you and your personal data?

A. Not much apart from my name, passwords and phone number
B. How I'm feeling, my best friends, family, music taste and a lot of other creepy stuff
C. They only know whatever I give them access to

3 Do you think it's fine that these companies have so much information on you?

A. Not at all. It violates my right to privacy
B. I don't really care
C. I'm completely fine with them knowing everything about me. I have nothing to hide

4 Have you ever thought about why search engines and social media apps are all free?

A. Nope! Doesn't figure in my life

B. Yes, I've definitely given it some thought

C. I've thought about it once or twice but then realized I have better things to do with my time

5 Do you know why social media companies give you their services for free?

A. Yes! They do it so that they can get personal information about me and use this information to target me with specific ads

B. They do it because they are generous

C. They do it because the government subsidizes them

6 Do you allow apps unnecessary access to your phone's data, like Instagram or Google Search asking for location access when it's not needed?

A. I don't allow apps access when it isn't required
B. I've noticed that some access isn't necessary to the app's functioning but I grant it anyway
C. I almost always allow any sort of permission access to my phone

7 Do you think your personal data can be used to influence people's actions?

A. Not at all. People can't be fooled that easily
B. Maybe a few people
C. Yes! I've heard of the Cambridge Analytica scandal where data was used to influence thousands of voters

JUSTICE adda

8 Do you think you're anonymous online?

A. Yes. I use a fake names and incognito mode when I'm on online forums so I can't be identified

B. I maybe identifiable to a certain degree but surely no one can figure out my entire life just by my online profile

C. I'm not anonymous online at all. Because I leave bits of personal information across a lot of sites. Put them all together and you could figure out a lot of my personal data

9 Is anyone listening in on your conversations?

A. Yes! Voice Assistants are constantly listening to you even if you don't call on them. This data is uploaded to company database and can be traced back to the individual

B. Nope. My conversations aren't that interesting

C. I don't really know but even if someone is then I don't mind

JUSTICE adda

10 Are you familiar with the phrase ‘data footprint’?

A. Nope! I’m not that into Sherlock Holmes

B. Crumbs of yourself you leave intentionally or unintentionally whenever you’re online in the form of cookies, location data and much more

C. Information about yourself you leave online with full knowledge of your actions

JUSTICE adda

ANSWER KEY

1	C	6	A
2	B	7	C
3	A	8	C
4	B	9	A
5	A	10	B

What is your data wokeness score?

DATA WOKENESS METER:

0-3 -> Sorry! You need to work on your data wokeness.

4-7 -> Not bad! You have a basic understanding of data and privacy but you still have a some way to go!

8-10 -> Oof, You've aced it!

JUSTICE adda

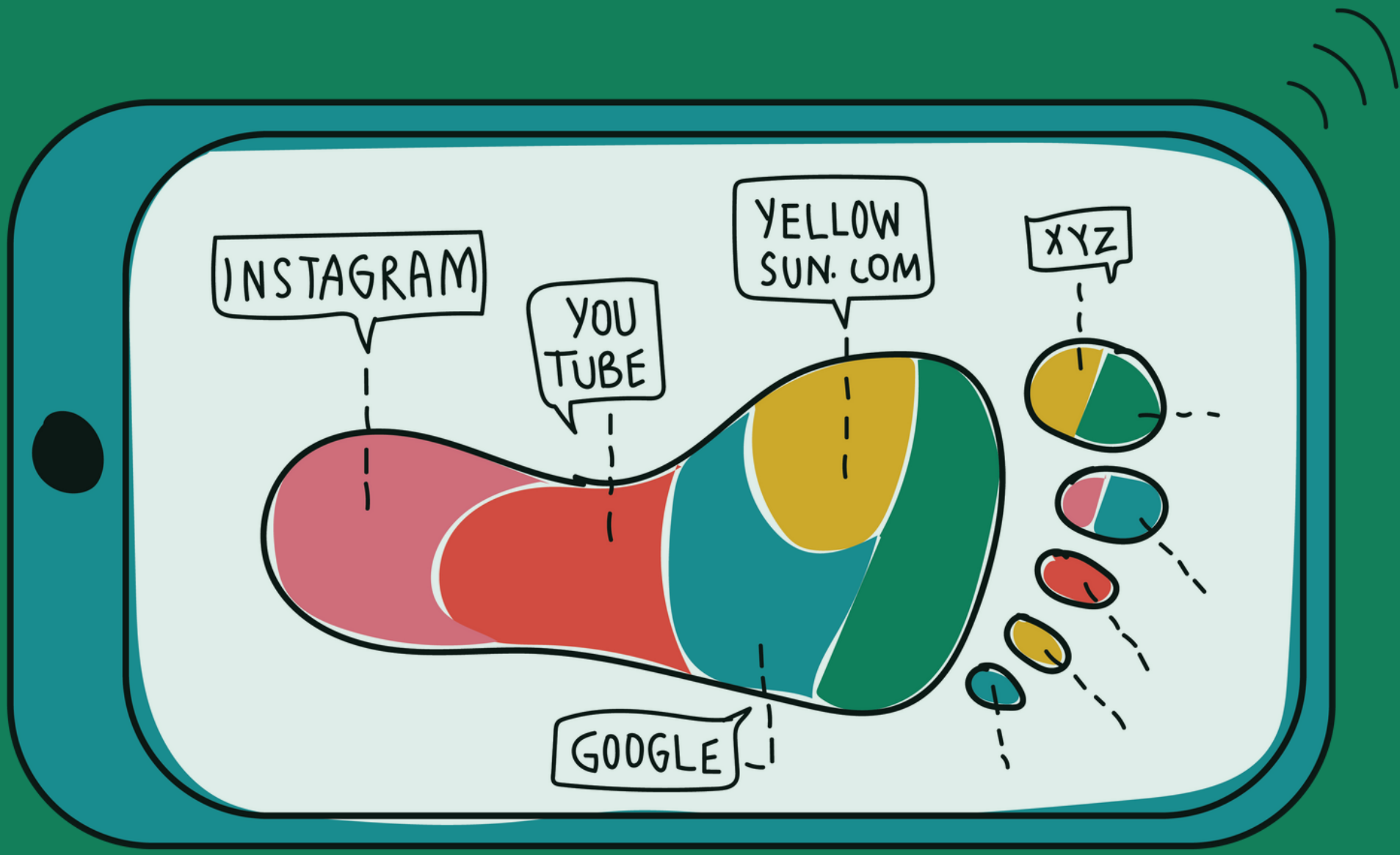
TRACKING MY DATA FOOTPRINT

MODULE 2

TRACKING MY DATA FOOTPRINT

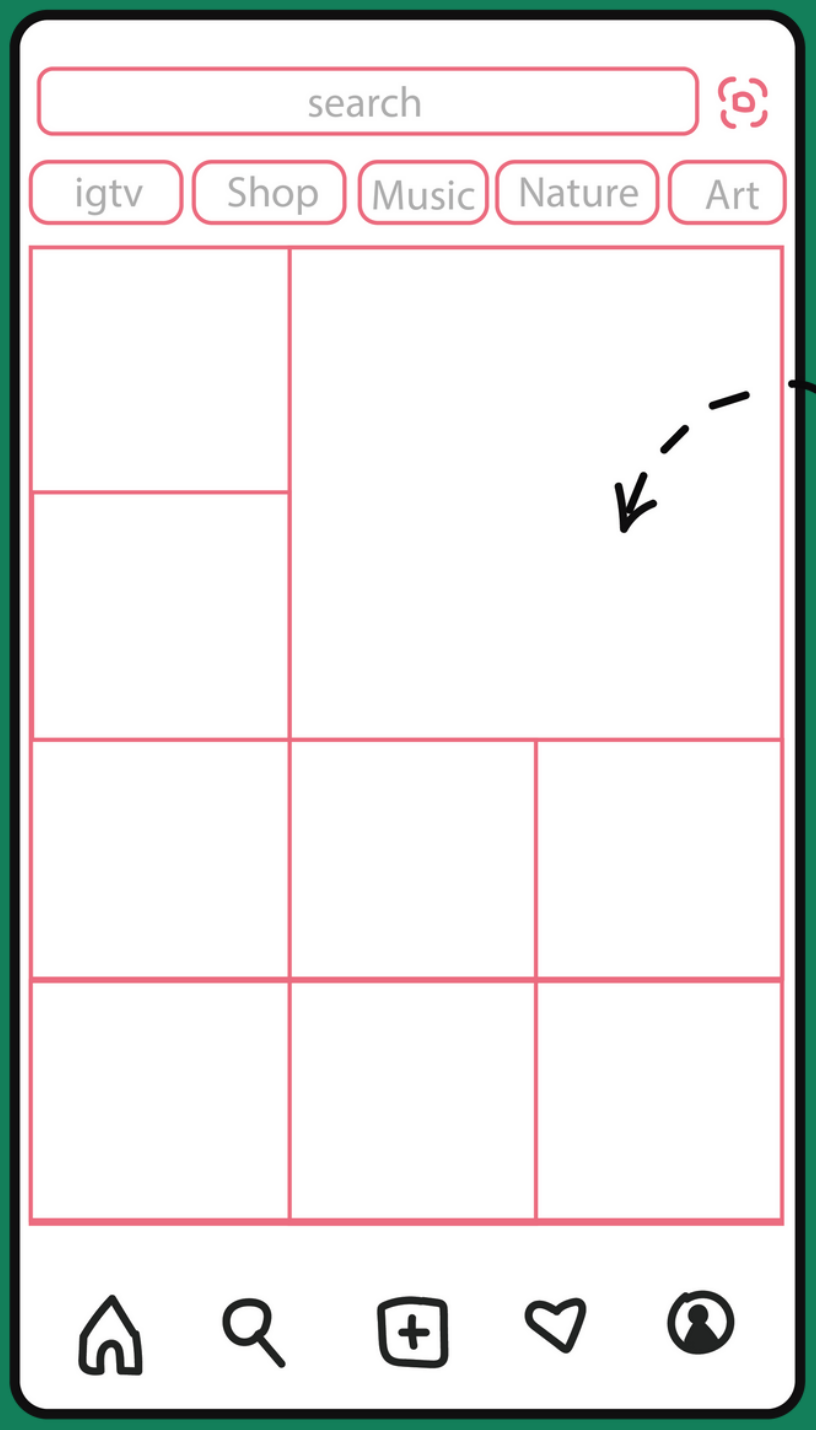
Remember the last question of the data wokeness quiz?
(Please go do the quiz in Module 1 if you haven't already!)

In this section we are going to break down your data footprint for you.



ACTIVITY 1

Sketch your Instagram explore feed and compare with your friends. What shows up for you?



ACTIVITY 2

- **Visit myactivity.google.com and go to Google Ad Settings to get a peek into how Google views you.**

  My Activity> Other Google Activity> Other Activity> Google Ad Settings

  Compare: Movies, music, relationship status, household income and where and what you study.

- **Also go to My Activity Homepage and make a note of non-Google apps being tracked.**

- **Give Google a score on 5 for how well it knows you.**

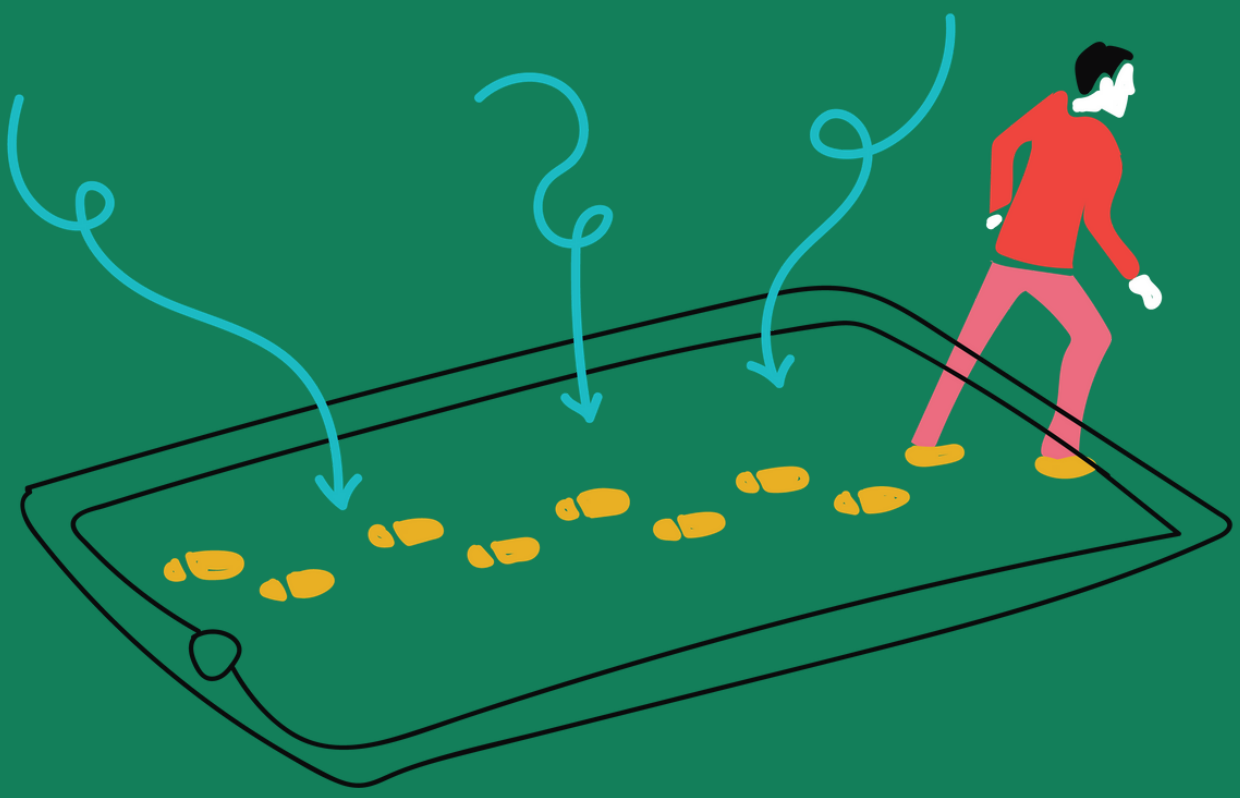
- **Check out the Data Detox Youth Kit by Tactical Tech for more such activities**

REFLECTIVE QUESTIONS

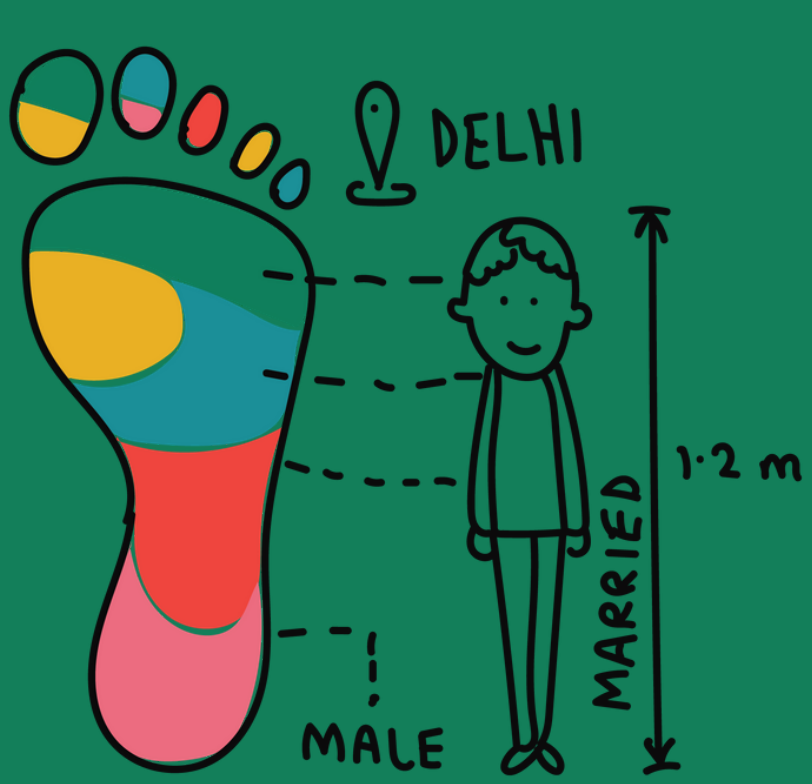
From the above activities, how is it that these companies know so much about you?

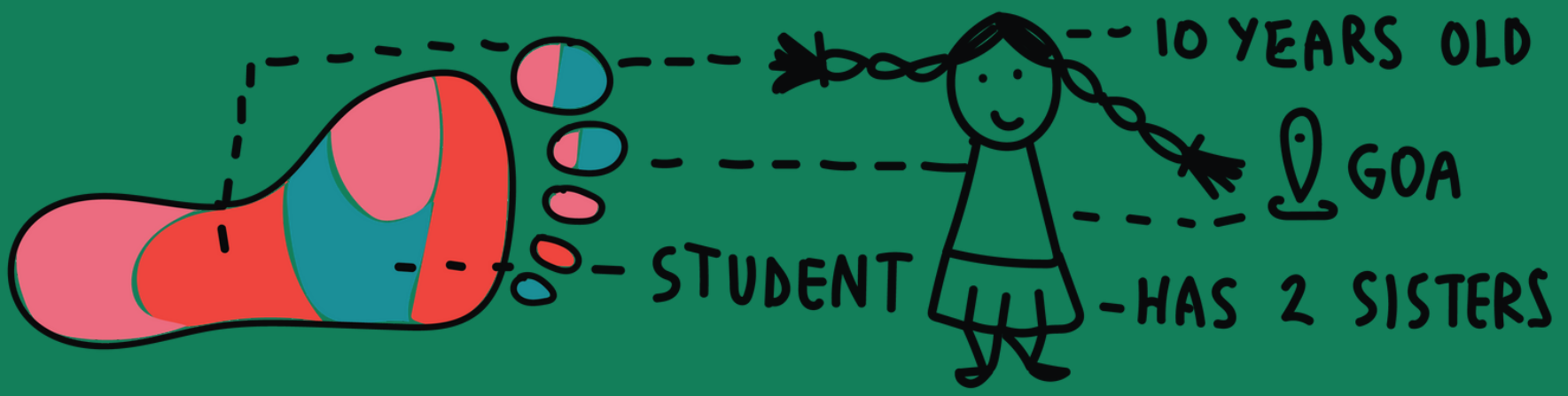
Because you're sharing it with them. They're picking up the crumbs that you leave scattered online and using it to create an image of you. These crumbs are your data footprint.

A data footprint is a set of traceable online activities that can be attributed to an individual.

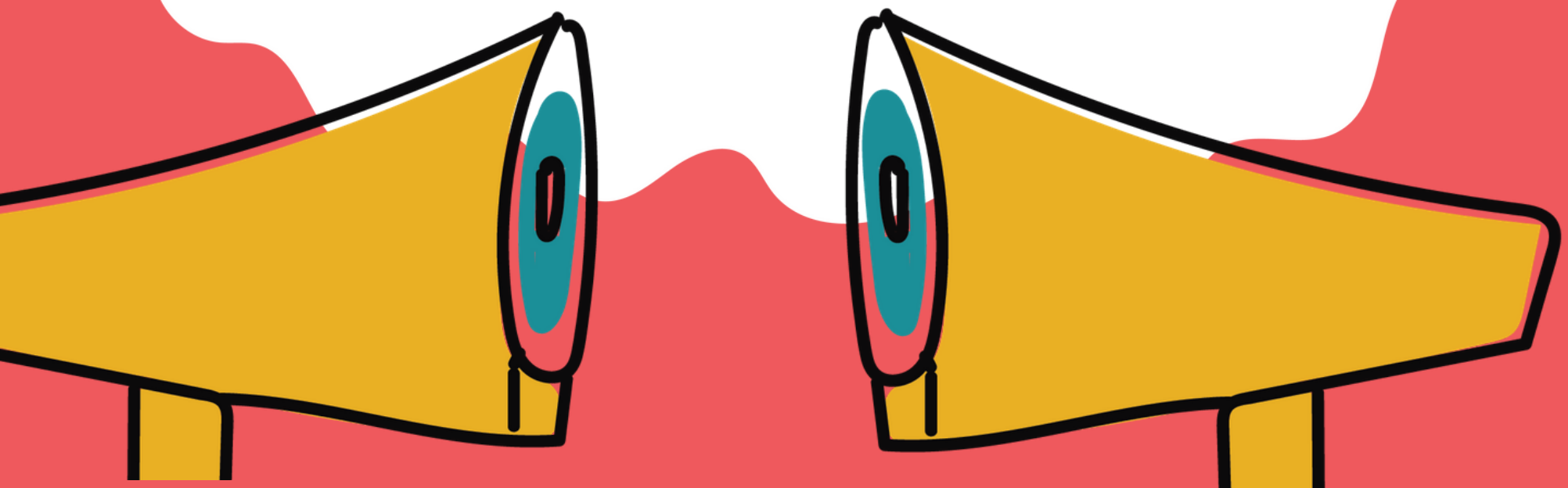


Using these footprints, individuals are profiled. This means that companies construct an image of you, based on the information you leave behind.





IMPLICATIONS OF MY DATA



MODULE 3

JUSTICE adda

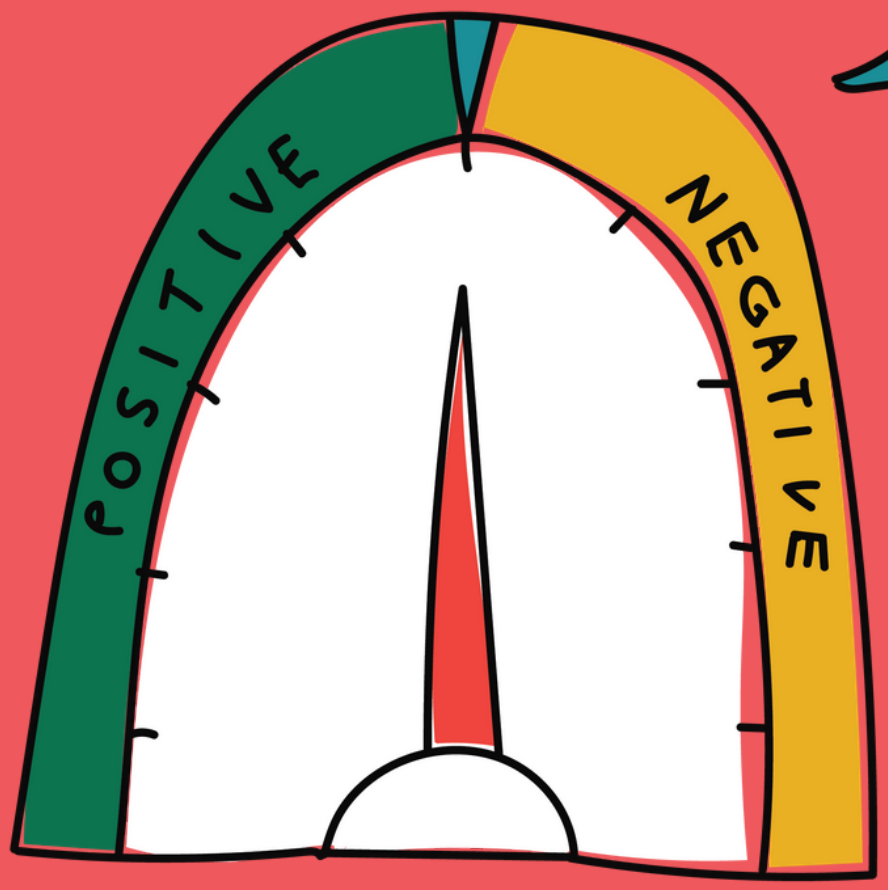
IMPLICATIONS OF MY DATA

Objective:

Why is it a problem that someone else has access to my data?

Time to break it down by looking at:

- **3A** Case studies
- **3B** An activity on data worth
- **3C** Privacy Gyan
- **3D** Data Puzzle
- **3E** Conclusion(ish)



3A. CASE STUDIES

So why is it a big deal that someone else has access to my personal data? Through these cases we will give you an overview of how data can be used against people to influence their actions and monitor them. The case studies are:

1. **Cambridge Analytica scandal**
2. **Algorithmic bias in courts**
3. **China's Social Credit system**
4. **The Aadhaar Project**

Cambridge Analytica Scandal

The Background: Cambridge Analytica was a British political consulting firm that was founded in 2013. It prided itself on being a pioneer in analysing people's personal data to help their clients win elections. Their clients included the Trump campaign in the 2016 US elections and the Brexit campaign to leave the EU.

The Controversy: Cambridge Analytica used Facebook as a base to analyze voter behaviour for the 2016 US election. They set up a quiz that 270,000 Facebook users took. The participants' data along with the data of people they were friends with subsequently got leaked, resulting in the company gaining access to 87,000,000 (that's million) profiles. All this was done right under Facebook's nose. This data (which included information like user's age, type of posts, level of education etc.) was used to classify them into categories in a process known as data profiling. Once people were profiled, they were sent targeted ads based on their personality types to influence the way they voted.

The Implications: This scandal fundamentally changed the way the public looked at data because for the first time, people could see the real-life effects of handing over their data to tech companies. This data proved to be so valuable that it had the potential to influence elections. No longer were its effects abstract.

The Lesson: Voter social media data is increasingly being used for political campaigns. Cambridge Analytica itself cannot be seen in isolation. Rather, it is just one instance of where such activities came to light. To know more about the interface of data and democracy, check out our Further Resources section.

JUSTICE adda

Machine bias and criminal law

The Background: In the US a tool called COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) was used in courts to assess the recidivism risk of criminal defendants, which is whether they would reoffend again. Based on the scores from this software, a judge could determine whether to detain a defendant. Those with high risk were often detained while awaiting a trial.

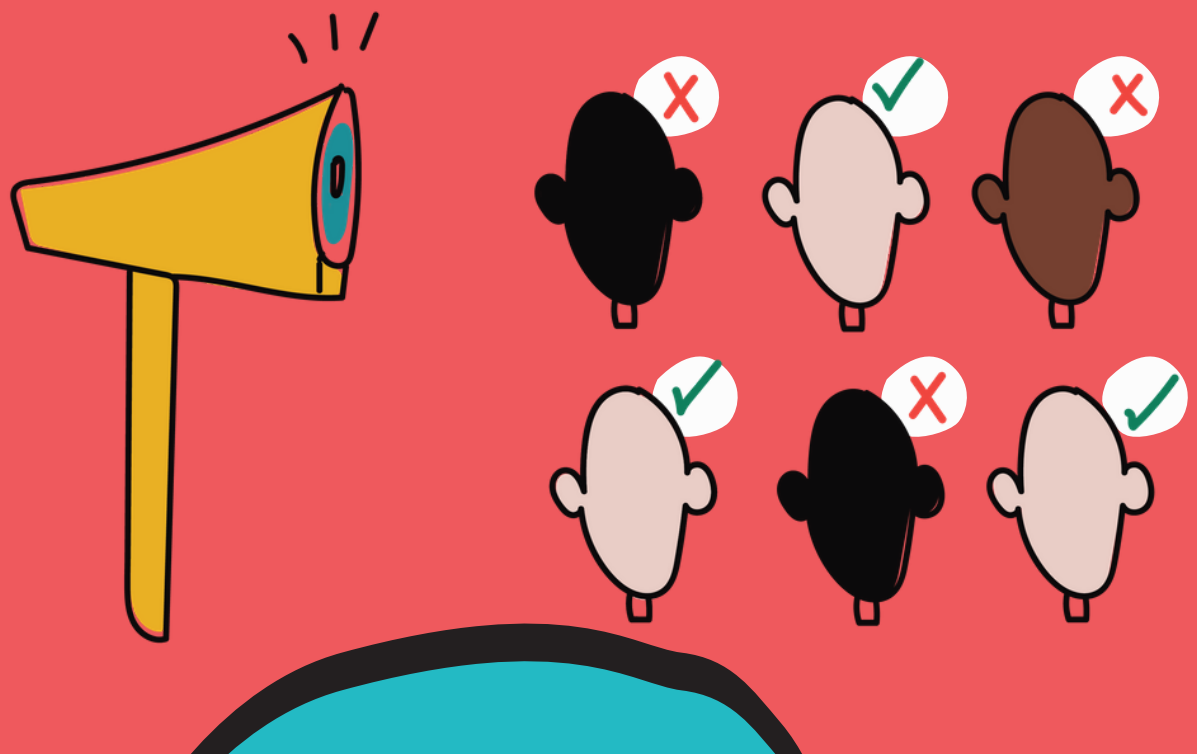
In a study by Pro Publica it was found that the software mislabeled black defendants as being twice as likely to be high risk of reoffending than white defendants- even though they didn't reoffend. White defendants on the other hand, were mislabeled at a low risk of reoffending- even though they did reoffend.

The Implications: This study raised questions about the data that was being used in order to compute these predictive scores, as well as the kinds of methodologies, that did not account for structural and racial discrimination.

The Lesson: In this instance it was clear that data can be used to discriminate against you.

Check out this resource by **Digital Empowerment Foundation on Data Rights for Communities** which will give you a background into how data is collected and processed, and the rights that users have.

In India, as Ameya Bokil, Avaneendra Khare, Nikita Sonavane, Srujana Bej and Vaishali Janarthanan have shown, technology is being used to implement caste based discrimination through biased police data, elaborate surveillance systems and predictive policing techniques. Do read the report here.



China's Social Credit System

The Background: China's Social Credit System is a scheme currently being developed. Its function is to provide every citizen with a social credit score to track the trustworthiness of citizens, corporations and government officials.

Each individual's score takes into account a person's actions when compiling the score. The higher the score, the better. Scores are calculated based on a combination of an individual's behaviour both on and offline.

Your online activity, from who your friends are, to the kind of websites you visit and what you post are all tracked. And from what we saw in Part 2- Tracking my Data Footprint (check it out if you haven't already!) , your social media can reveal A LOT about you. This is combined with China's close public monitoring and facial recognition systems and government data to give you a score.

Some things that could lower your score are:

1. Jaywalking
2. Not paying your bills or employees on time
3. Playing music too loud in public
4. Buying and playing too many video games
5. Social media posts that go against the Chinese government

In contrast, actions such as giving to charity, paying bills on time and following public laws can increase your score.

The Controversy: The score essentially seeks to reinforce 'good' citizen behaviour. Low scoring individuals are blacklisted and lose access to services such as air and train travel, buying property and getting loans. On the other hand, higher scores get you tax cuts, better rental rates and faster foreign visas.

The Implications: This system relies heavily on data profiling to work. Millions of data footprints are used to build an image of you. Your level of access to services therefore depends on your profile.

What is also truly worrying is the fact that none of the technologies that China is using is new.

The System Currently: The system so far has been decentralized and conducted by various public and private partners in different cities across China. Each city has different scoring systems, criteria, rewards and punishments. The more centralized system that was supposed to be launched in 2020 was halted because of the Covid-19 pandemic. As of yet, the fully formed system remains to be seen.

However, this hasn't stopped these various systems from collectively covering and ranking over 1,020,000,000(that's billion) individuals.

Of these, more than 25,000,000 (that's million) individuals have already been restricted from air and rail travel.

The challenges of surveillance and digital freedom, are a serious problem in **India** as well.

The Centre For Internet and Society have a series of reports that examine digital freedom including on questions of internet shutdowns, censorship and on questions of privacy and data protection. For more on this please click here.

The Internet Freedom Foundation has a project called Project Panoptic that looks at Facial Recognition Systems in India which can be access here.

The Lesson: This case tells us a how data can be used to restrict freedoms.

The Aadhaar Project

The Background: Aadhaar is a 12-digit identity number that is available to citizens and residents of India. Biometric information- like the individual's ten fingerprints and iris scan- are combined with demographic details to generate this unique number. Aadhaar initially introduced so that it would serve as an identity card for those who had no other official government identification. Individuals who possessed other identification such as PAN cards and passports wouldn't need it. Despite being completely voluntary, the Indian government- since the scheme's inception in 2009- has consistently pushed to make Aadhaar mandatory to receive scholarships, open bank accounts, access Public Distribution Systems (PDS) etc.

Six years after Aadhaar was introduced by notification, the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act of 2016 was introduced.

The Controversy: Although by no means the only issues, Aadhaar has come under criticism for three things: a lack of privacy, function creep and Aadhaar-Based Biometric Exclusions.

Privacy: While there are a host of privacy issues with Aadhaar, the one we're choosing to focus on is the integration of your personal data. As we've seen from the above modules, your data is constantly being collected by interested parties. Each time you visit a website, you leave different bits of information behind (See the Data footprint). A travel website may know where you want to go on holiday but it doesn't know if you can afford it. This information is exclusive to your bank's website, which in turn, doesn't know what your holiday preferences are. The only one who has the full picture of your finances and where you want to vacation is you.

By linking your sensitive biometric information- that the government has access to- with bank details, phone numbers, travel history, employment details etc. Aadhaar integrates this previously scattered information, which can be used to profile you.

Function Creep: This connects to the second aspect of the function creep in the use of the technology. This means that while Aadhaar as a technology was intitally set up for one purpose, it has been expanded to new areas, much beyond its original intent. It is now not just a matter of providing identity or de depulication of the population but also for admission to schools, rations, mid day meals among other things, and it has entered more and more aspects of our lives.

ABBA: One of the main reasons for Aadhaar was that it would reduce corruption and leakages in India's Public Distribution Systems (PDS). The old system relied on vulnerable households being given a ration card which would then be used to claim grains and other essentials at subsidised rates.

The introduction of Aadhaar-Based Biometric Authentication (ABBA) was thought to deal with issues such as card theft or loss. Individuals would have to link their Aadhaar to their ration cards and do a fingerprint scan every time they needed to buy provisions. However, this new system has created new problems, instead of trying to solve the old ones. Firstly, by making Aadhaar mandatory for accessing entitlements, those that don't have these cards are immediately being excluded. Further, biometric authentication is done through a Point of Sale (PoS) machine, which matches the individual's fingerprints against what's stored in the Aadhaar database. This exercise however, requires a strong, stable internet connection- which much of rural India lacks. There are also frequent issues with fingerprint authentication as many people engaged in manual labour have extremely worn out prints. There are also issues with the PoS machine itself, depriving many as a result. To get a better idea of how entitlements accessed under the new system, head over to Day 5 of our Data Diet module. For more information, also check out our Further Resources section.

The Lesson: This case tells us how data and identity can be used to govern your interactions, as well as be used to deny access to services.

3B: ACTIVITY

Have you ever wondered how much your data is worth? Discuss with your friends and write estimates of how much you think your personal information is worth in the space provided below.

Then go to this Financial Times Resource (Available Here) to find out the real value. Compare with friends.

Reflect on the fact that while your individual personal data is being sold for so little, the top 5 tech companies in the world (they owe a significant portion of their wealth to their user's data), who are profiting off of it, are worth over 5,000,000,000,000 (that's trillion) dollars.

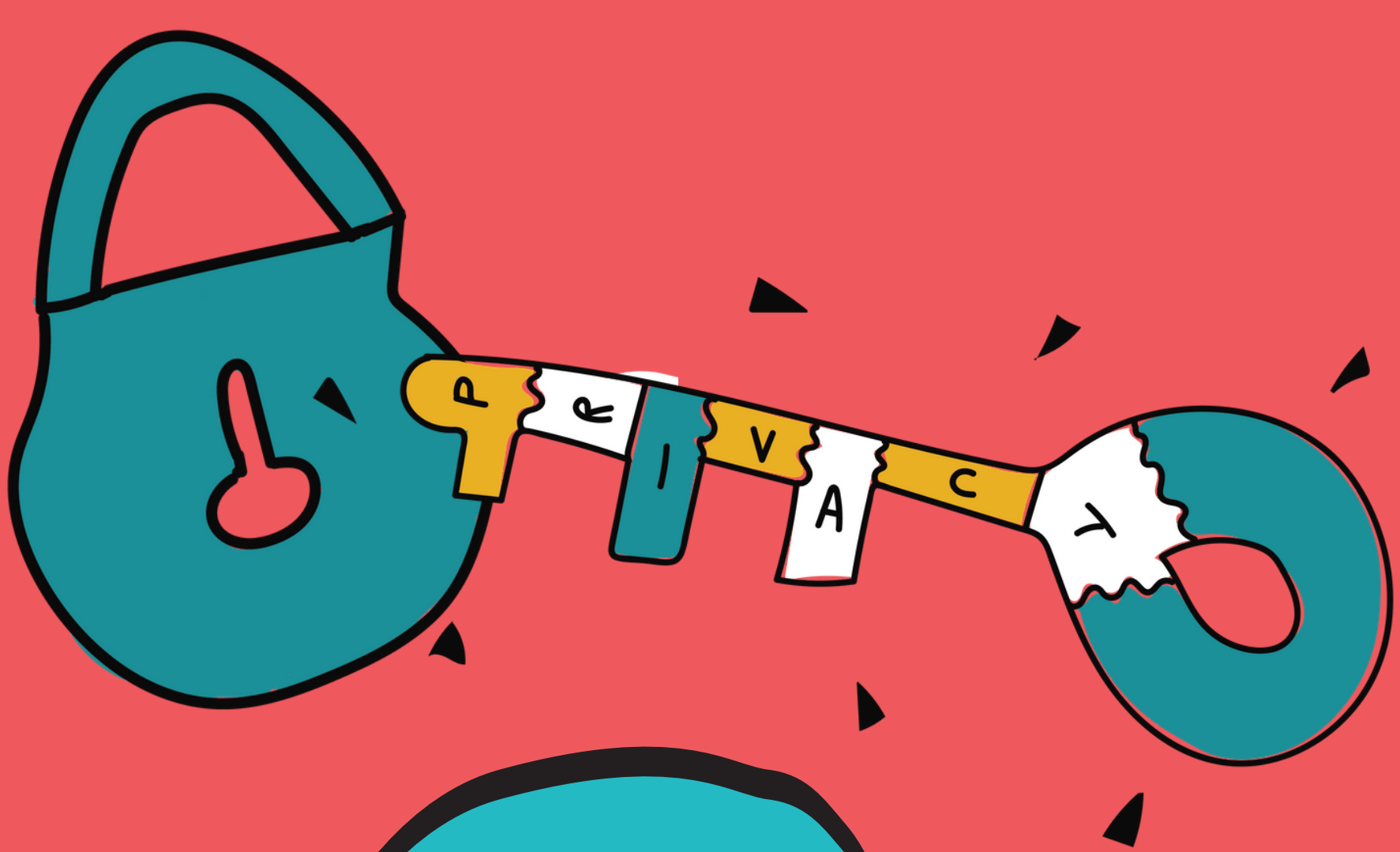
To put that into context, the data industry has now become more valuable than oil. Our data has become a seemingly unlimited resource to extract and profit from.

What do you think the solution to this is? Do we need more regulation? Or is this extraction fine as long as companies make people aware of what they're doing and pay them for their personal data?

3C: PRIVACY GYAN

You know now that your data has a real-world impact on you and the community around you; but what are some of the more general or textbook reasons about why privacy should matter to you?

Well, we've come up with a key in which you can remember these reasons.



P-> Personal. My data is my information. I don't want strangers looking at it and making money off it.

R-> Regulation. Since my online data is so vital to me, it's important it's protected by the government by strict data regulation laws.

I-> Intelligence. As computer systems and profiling becomes more and more advanced, it is essential that you learn about how these systems work and are given an explanation for their functioning.

V-> Virtual Private Networks and other tools that can be used to protect my data.

A-> Algorithmic Bias. Computer systems aren't perfect and tend to perpetuate biases and stereotypes present in society.

C-> Cloak (fancy way of saying hide) your data from prying eyes.

Y-> Yours. Take back control of your own data.

Think of how you can speak to people around you about why data and privacy matters.Come up with a couple of dinner table conversations that you could have with family, friends or your community on knowing more about data.

If you want some ideas, check out the Digital Defense Playbook from Our Data Bodies available here. It has resources on how to do a data body check up, and build community defense approaches.

If you want to learn how to work with data, check out the resources on Data Basic available here.

3D: DATA PUZZLE

We've created a short exercise to help you remember important privacy-related terms!

Personal data: Any information that could be used to identify an individual, including digital information

(Data) footprint: Traceable online activities that can be used to identify an individual

Cookies: Information about a user that is stored in their computer by a web browser

Consent: To give permission for something to happen. As a personal rule, nothing should happen with your personal data without your knowledge and understanding

Profiling: In the context of social media, it means building a virtual image of a person and their characteristics based on their online information

VPN: Virtual Private Networks are more secure ways of browsing the internet. They essentially create secure connections between devices to prevent hacking or spying

Incognito: It means concealing your identity. Every browser comes equipped with incognito mode. When activated, your history, site data and cookies aren't saved

Extensions: Downloadable software that you can attach to your browser to customize usability

Terms (of service): Lengthy legal agreements between a service provider and an individual. It is here that social media companies specify how much they track you, but they're too lengthy and convoluted to read (unless you're a lawyer)

Hackers: People constantly trying to get your data!

Surveillance: Close monitoring of someone. With the rise of social media, it is becoming increasingly easy to track individuals because their information, from where they are to who they talk to, is available online.

Password: It is very important to have a strong password! Please don't use the same password for all your accounts!

Cache: Cached data is information from a website that is stored on your computer so the next time you use the website, it can load faster. Unlike cookies, they don't store personal information. They just store website information.

JUSTICE adda

Find the words in the puzzle

G	N	I	L	I	F	O	R	P	O	D	A	C	H	P
E	H	C	A	C	S	T	X	T	Y	T	U	O	A	A
Y	X	I	B	F	Y	F	I	Q	A	O	C	N	C	S
K	V	S	A	P	V	N	M	D	T	L	S	S	K	S
F	V	L	T	N	G	J	L	Q	A	M	B	E	E	W
K	Y	K	O	O	B	A	A	M	N	W	Y	N	R	O
N	O	A	C	Z	N	V	E	C	J	Q	Q	T	S	R
K	F	N	N	O	G	Q	D	I	O	X	B	P	N	D
V	I	G	S	P	L	Q	H	S	N	O	L	L	X	Z
K	G	R	V	V	V	C	J	F	M	X	K	U	K	Z
F	E	D	A	T	A	F	O	O	T	P	R	I	N	T
P	E	X	T	E	N	S	I	O	N	S	P	D	E	Z
E	C	I	V	R	E	S	F	O	S	M	R	E	T	S
H	S	U	R	V	E	I	L	L	A	N	C	E	C	Z
F	I	G	X	E	U	C	U	H	J	E	A	C	Q	Z

cache consent datafootprint termsofservice
extensions incognito password personaldata
profiling surveillance vpn cookies hackers

3E: A CONCLUSION(ISH)

So if you've stayed with us from Module 1 or joined us midway, Congratulations! You've made it this far with a lot of new information, and that's no small feat!

So why are we telling you all this? What's the point behind this entire module? Think about it for a second and look at your explanation when you're ready.

The point isn't that you shouldn't use your phone, that social media is a bad thing, or that you need to feel guilty about granting permissions to apps on your phone.

The point is that you need to be more informed about your data and how it can be used against you.

It is about creating awareness so that the next time an app asks you for a permission or your government asks you for data, you'll think twice and ask yourself, "Is this really necessary?"

It is important to realise that Digital Rights are Human Rights whether in terms of privacy, health, education or the right to a fair trial. Check out this resource from the Digital Freedom Fund which details the importance of human rights for the digital age here.

JUSTICE adda

DATA DIET

MODULE 4

JUSTICE adda

DATA DIET

Now that you have a basic idea of what you can do to protect your data, let's set in a routine. This routine (or Diet) will help you learn about what you can do long-term to protect your data.

Our Data Diet is a 5 day program that has three elements consisting of Something to Do, Something to Give Up and Something to Learn. The idea is to find simple ways in which we can build a more healthy and balanced data diet.

JUSTICE adda

OVERVIEW OF DIET

Something to Do

Start Afresh: Clear browsing data and use incognito

Something to Give Up

Cleanse MyActivity: Go to MyActivity and turn-off Youtube, Webpage and Location history from being stored. Also turn off ad personalisation

Something to Learn

Round the Clock Tracking: Watch a video on how we are constantly being tracked

JUSTICE adda

DAY 1

Something to Do

Start Afresh

On Chrome:

1. Go to Settings
2. Go to Privacy and Security
3. Click ‘Clear Browsing Data’
4. Choose the advanced option and choose what to delete. Make the time range the last 7 days

Use Private Browsing after clearing data

Personal Browsing Mode:

Check out a project by Tactical Tech called Me and My Shadow for more advice on customizing Chrome to not track you.

Additionally, you can customise your browser to not allow third party tracking on incognito mode.

JUSTICE adda

Something to Give Up

Cleanse MyActivity

DAY 1

1. Go to myactivity.google.com
2. The first things you'll see are three boxes that say 'Web and App Activity, Location History and YouTube History.'
3. Click on them at a time
4. For Web and YouTube History, you'll need to click on saving Activity and then turn off the blue marker
5. For Location History, you can see the turn off option right after you open it
6. This will pause Google from collecting and storing your data
7. Alternatively, you could choose the auto-delete option under each of these three categories and choose an auto-delete time that works for you

JUSTICE adda

Something to Give Up

Cleanse MyActivity

DAY 1

8. Go back to the home page and go to Other Google Activity (on the left)-> Other Activity-> Manage Ads Settings-> Turn off ads personalisation. Also open the drop down menu and unselect the ticked box on personalized ads.

9. To find out more about myactivity and the kind of information Google has on you, check out the activity in Module 2: Tracking My Data Footprint

JUSTICE adda

Something to Learn

Online Tracking

DAY 1

Watch this video by Deutsche Welle on how all of us are constantly being tracked online.

How you are being tracked in the web | Online Tracking explained

What does all this tracking mean in terms of the profiles that are generated about you?
Go back to our section on machine bias and criminal law in Module 3 to look at how profiling reflect our biases.

JUSTICE adda

OVERVIEW OF DIET

DAY 2

Something to Do

Alternatives: Go through this list of alternative apps and download what works for you

Something to Give Up

App Permissions: Rethink about what apps you need

Something to Learn

Other Alternates: Watch a video on alternative apps

JUSTICE adda

Something to Do

Alternatives

DAY 2

Go through our list of alternative apps and download what works for you.

Privacy Badger: A browser ad-on that prevents advertisers and other third parties from tracking where you go and what websites you access. To learn more, visit their website here.

DuckDuckGo: An alternative search engine. DuckDuckGo does not profile users and send them targeted ads. You can learn more about them on their website here.

Mozilla Firefox: Firefox is an internet browser. It's privacy oriented (the organisation itself is a non- profit) and monitors and blocks third-party cookies.

JUSTICE adda

Something to Do

Alternatives

DAY 2

VPNs: A Virtual Private Network (or VPN) creates an encrypted connection (or tunnel) between you and the internet, allowing you to stay anonymous. Advertisers will have a harder time tracking you across sites and selling your data.

Since there are a lot of VPNs to choose from (some offer paid subscriptions), take a look at the ones available on PC Mag here.

Of course, these are just some alternatives. To get a more extensive list of alternates for Maps, Gmail and Meet, check out Tactical Tech's Data Detox Kit's Alternative App Centre here.

JUSTICE adda

Something to Give Up

App Permissions

DAY 2

We all have to deal with apps constantly asking us for permissions and most of the time, we give in to them. However, it's important that we ask ourselves WHY. Why does this particular app need access to my phone's features?

Unfortunately, we can't provide a guide on how to evaluate each and every app. All we can say is, remember you are not obligated to give out data to apps that don't need it.

For example, it's fine if a Maps App requests your location when you're using the app but is it okay to accept that same request when Social Media App asks you?

JUSTICE adda

Something to Give Up

App Permissions

DAY 2

On your phone, Go to Settings->Apps and Permissions-> App Permissions

Go through individual app permissions and turn off anything that isn’t needed, like unwanted intrusions on location data, contact information or body sensors.

Also go through Tactical Tech's Data Detox Kit for tips on how to improve basic phone privacy here.

JUSTICE adda

Something to Learn

DAY 2

Watch this great video by All Things Secured on reducing your reliance on Google Products:

https://www.youtube.com/watch?v=6ziYwwuNmns

OVERVIEW OF DIET

Something to Do

Take back control of your cookies

Something to Give Up

Clear your Cookies: Set a reminder on your phone to go through and clear your cookies once every week

Something to Learn

The Problem with Cookies

JUSTICE adda

Something to Do

Take Back Control of your Cookies:

DAY 3

1. On Chrome: Go to Settings-> Privacy and Security-> Cookies. Select the Option ‘Block Third Party Cookies.’ This will prevent you being tracked and profiled across sites. Also select the ‘Do not Track Request’ option. This requests websites not to track you, although they are not obligated to comply.

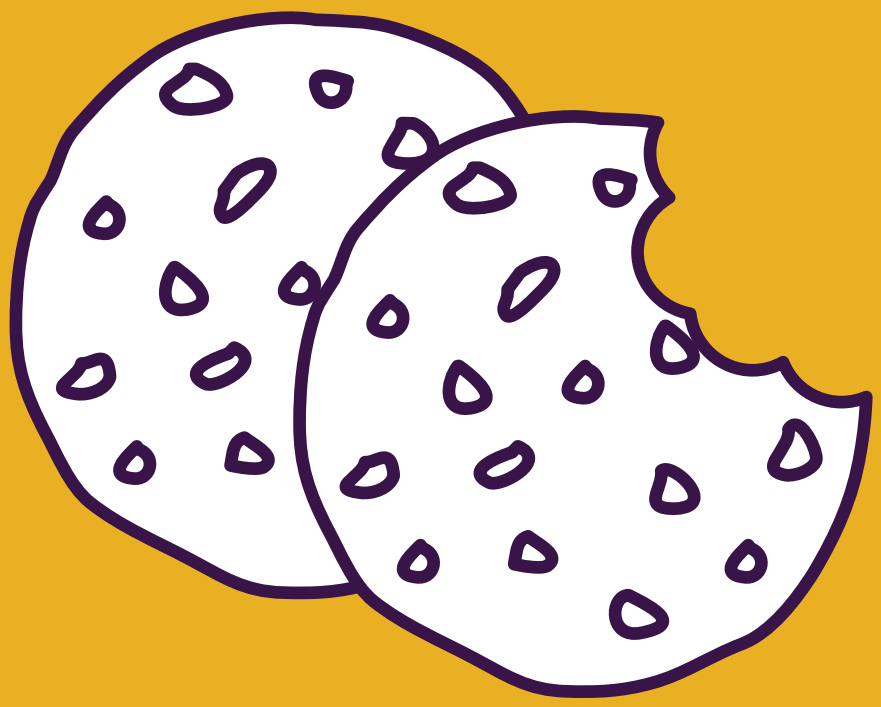
2. On Firefox: Go to Settings-> Privacy and Security-> Enhanced Tracking Protection-> Custom. Select Tracking Content, Cryptominers and Fingerprinters. Under Cookies, choose the ‘All Third Party Cookies’ option.

JUSTICE adda

Something to Give Up

DAY 3

Set a reminder on your phone to go through and clear your cookies once every week



JUSTICE adda

Something to Learn

The problem with Cookies

DAY 3

But wait, what are cookies? Unfortunately, cookies online aren't nearly as nice as they sound! They are essentially information about you that is gathered and stored on your browser every time you visit a website. Only that particular website has access to the cookie.

Some of these are helpful. For example, when you open your email on your browser you're already signed in because the website stores your password in the form of cookies that keep you logged in.

However, they are also problematic as third party cookies are used to track user activity across different sites. This is why when you look for phones on Amazon, you later see phone ads on other websites.

The Good News: Cookies are stored in your browser, which means you can restrict them.

JUSTICE adda

OVERVIEW OF DIET

Something to Do

Instagram Feed Exercise

Something to Give Up

WhatsApp: Give up Convenience

Something to Learn

Filter Bubbles

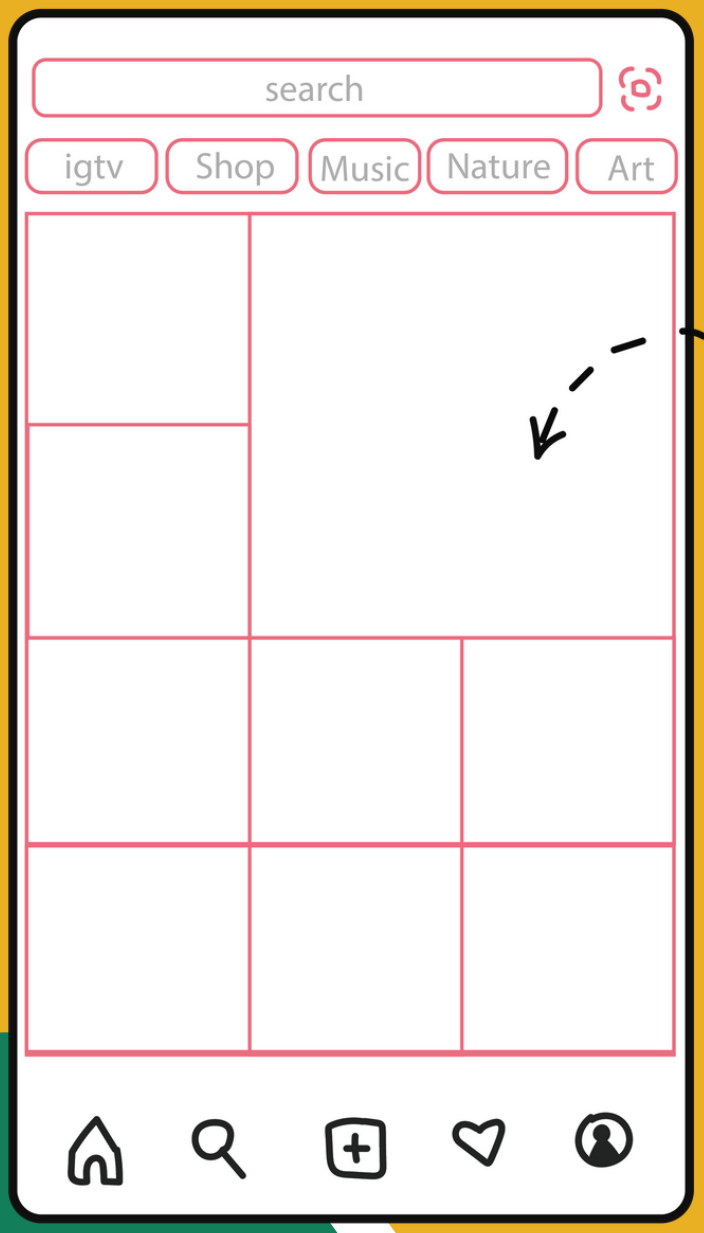
JUSTICE adda

Something to Do

Instagram Feed Exercise

DAY 4

Visit Module 2: Tracking my Data Footprint and do the Instagram exercise.



JUSTICE adda

Something to Give Up

WhatsApp: Give Up Convenience

DAY 4

Why are the recent changes to WhatsApp's privacy policy problematic for your data? Check out Internet Freedom Foundation's article on this here.

JUSTICE adda

Something to Learn

Filter Bubbles

DAY 4

Check out this article on Filter Bubbles from the Reuters Institute on how social media algorithms curate your content based on stories or posts you're already clicking.

OVERVIEW OF DIET

DAY 5

Something to Do

How the Internet is becoming increasingly indispensable in our daily lives

Something to Give Up

My Data and Surveillance

Something to Learn

A Public Distribution Maze/Mess

JUSTICE adda

Something to Do

DAY 5

How the Internet is becoming increasingly indispensable in our daily lives

Imagine someone gave you the choice between choosing food, the internet, shelter, clothing, employment or your mobile phone. What would be your first choice? What would be your second? Rank these six things in order of preference and write a brief line or two on your reason behind each rank.

Now, read Digital Empowerment Foundation's piece on the importance of the internet in people's lives here.

Reflect on the importance of internet in people's lives (and yours) and how this gives undue power with those in control of the it.

(Hint: think along the lines of the internet being owned and controlled by fewer parties unlike those other resources).

JUSTICE adda

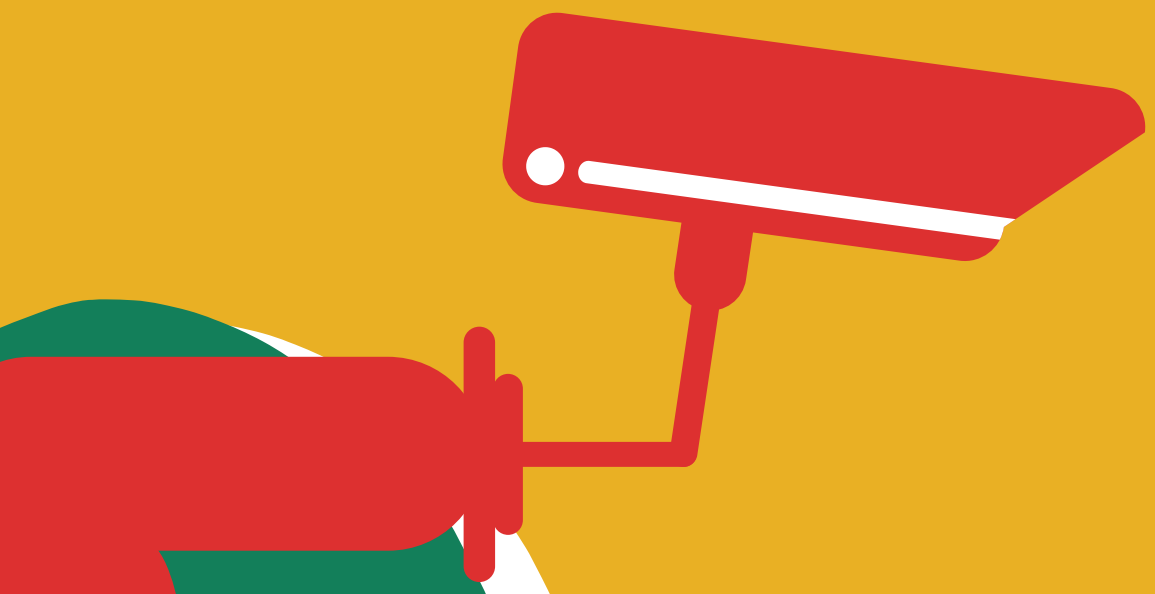
Something to Give Up

My Data and Surveillance:

DAY 5

Stop giving up unnecessary data over to the government. To learn more about the extreme repercussions of governmental control over personal data, read the piece on China's Social Credit System in Module 3: The Implications of my Data.

Have you checked out Project Panpotic by Internet Freedom Foundation, or the resources from Centre for Internet and Society ? If not, go back to the case studies for more on this.



JUSTICE adda

Something to Learn

Public Distribution System Maze/Mess:

DAY 5

Personal data (through Aadhaar) is playing a critical role in welfare and Public Distribution Systems. By tying Aadhaar to rations, people are forced to overturn excessively private data over to the State just for the sake of subsistence.

However, a lot of the time, these electronic systems aren't implemented properly, resulting in rations being withheld due to technical glitches. Check out this activity to find out more about rations and their inaccessibility from India's poorest in this Economic and Political Weekly article available here.

To know more about concerns surrounding Aadhaar, visit Module 3 of the workbook.

JUSTICE adda

FURTHER RESOURCES

MODULE 5

JUSTICE adda

FURTHER RESOURCES

This section includes the following:

1. **Links to extra reading and video material**
2. **Google Sheet to track and compare data footprint**

Cambridge Analytica

Vox

The Great Hack

The New York Times

Click on the icons to read or watch videos on the given topic.

Aadhaar

The Wire

EPW

EPW

Rethink Aadhaar

Click on the icons to read or watch videos on the given topic.

Black Mirror

Algorithmic Bias

Brookings

Propublica

Click on the icons to read or watch videos on the given topic.

Algorithmic Bias

TNI long reads

Centre for Internet and Society

Centre for Internet and Society

Click on the icons to read or watch videos on the given topic.

JUSTICE adda

Data and Democracy

Data Detox Toolkit

Access Now

Cookies

Create a Pro Website

Click on the icons to read or watch videos on the given topic.

Location Tracking and Contact Tracking

New York Times

Centre for Internet and Society

Data Regulatory Policies

GDPR

EPW

Click on the icons to read or watch videos on the given topic.

State Surveillance

Wired

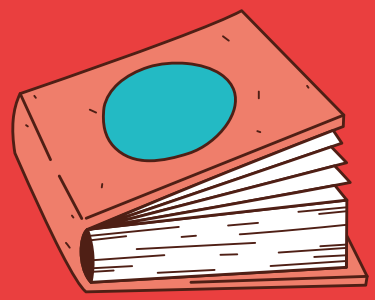
South China Morning Post

Wired

Digital Freedom Fund

Wired

Centre for Internet and Society



Project Panoptic

Click on the icons to read or watch videos on the given topic.

Browsers

Washington Post

Strong Passwords

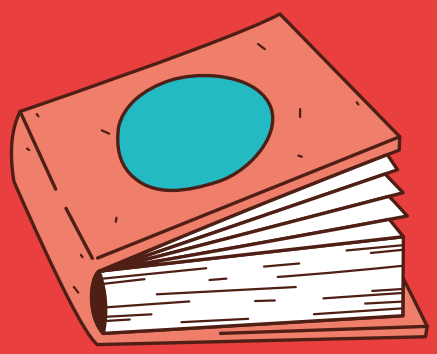
Avast

Click on the icon to read on the given topic.

Data Footprint

Data Detox Kit

Conversations Around Data



Our Data Bodies

DataBasic

Click on the icon to read on the given topic.

JUSTICE adda

This resource has been been conceptualised, written and designed by Ravi Mathews, Siddharth deSouza and Sharada Kerkar.