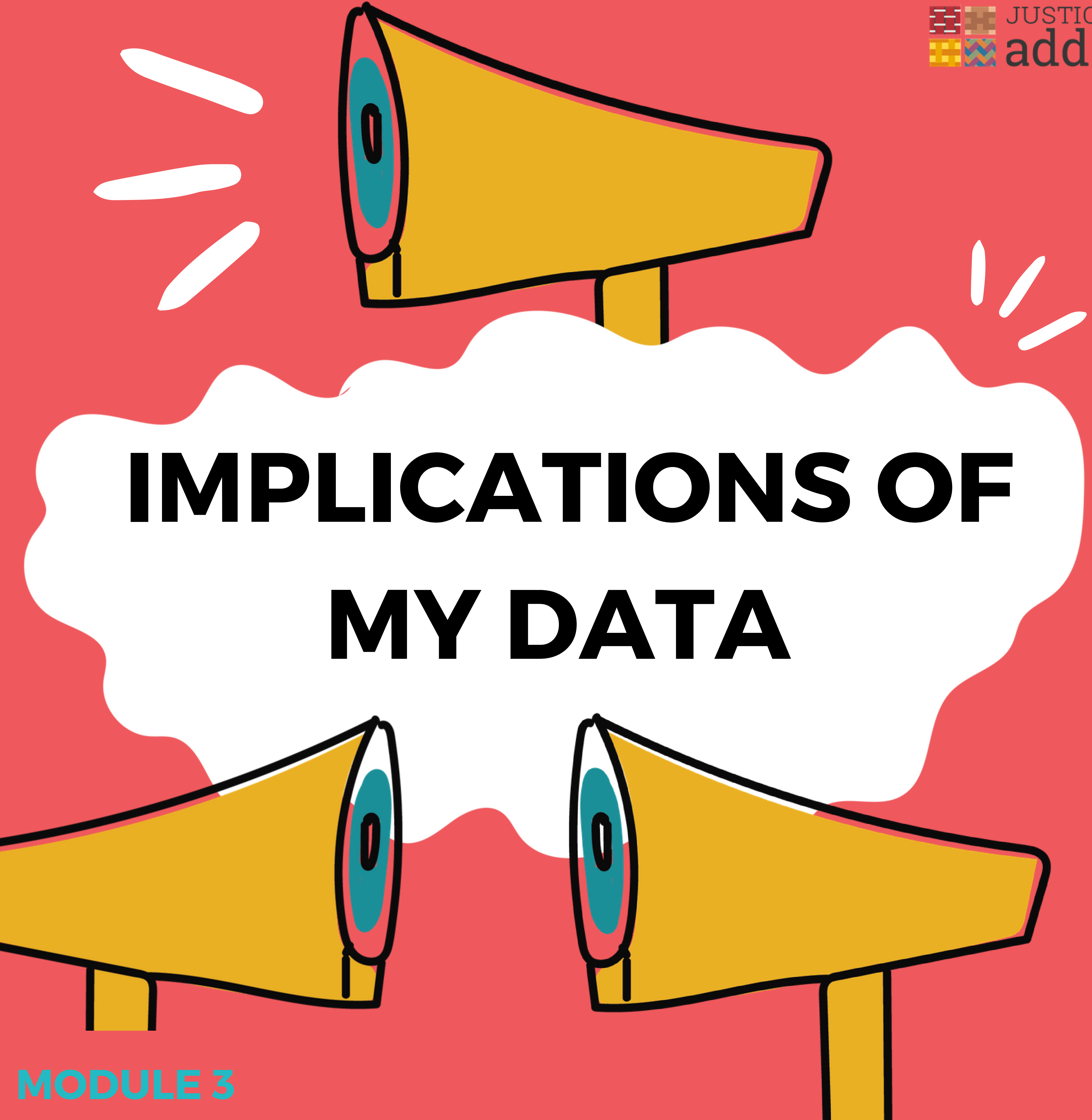
JUSTICE adda



IMPLICATIONS OF MY DATA

MODULE 3

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:

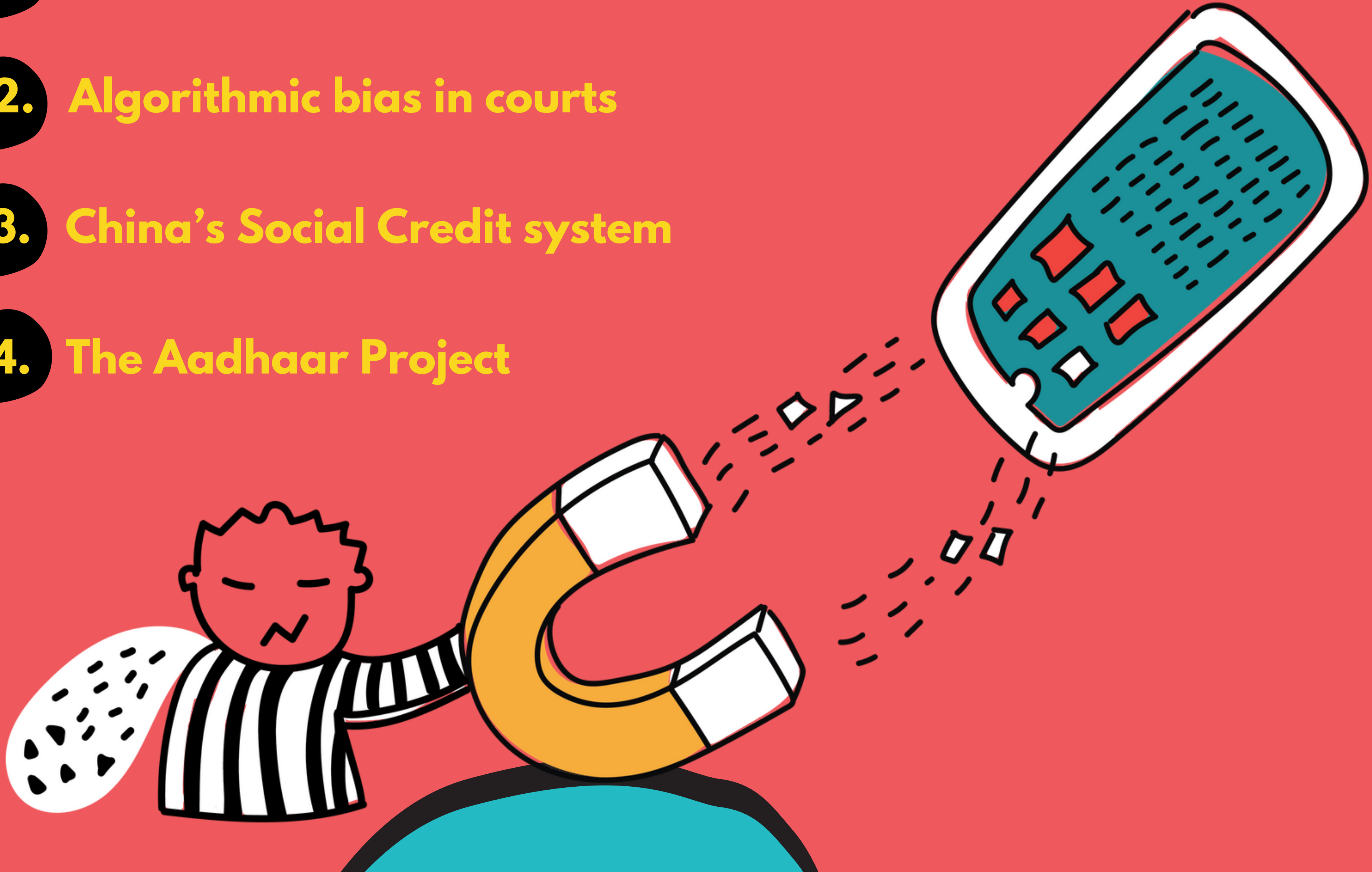
- **3A** Case studies
- **3B** An activity on data worth
- **3C** Privacy Gyan
- **3D** Data Puzzle
- **3E** Conclusion(ish)

JUSTICE adda

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.

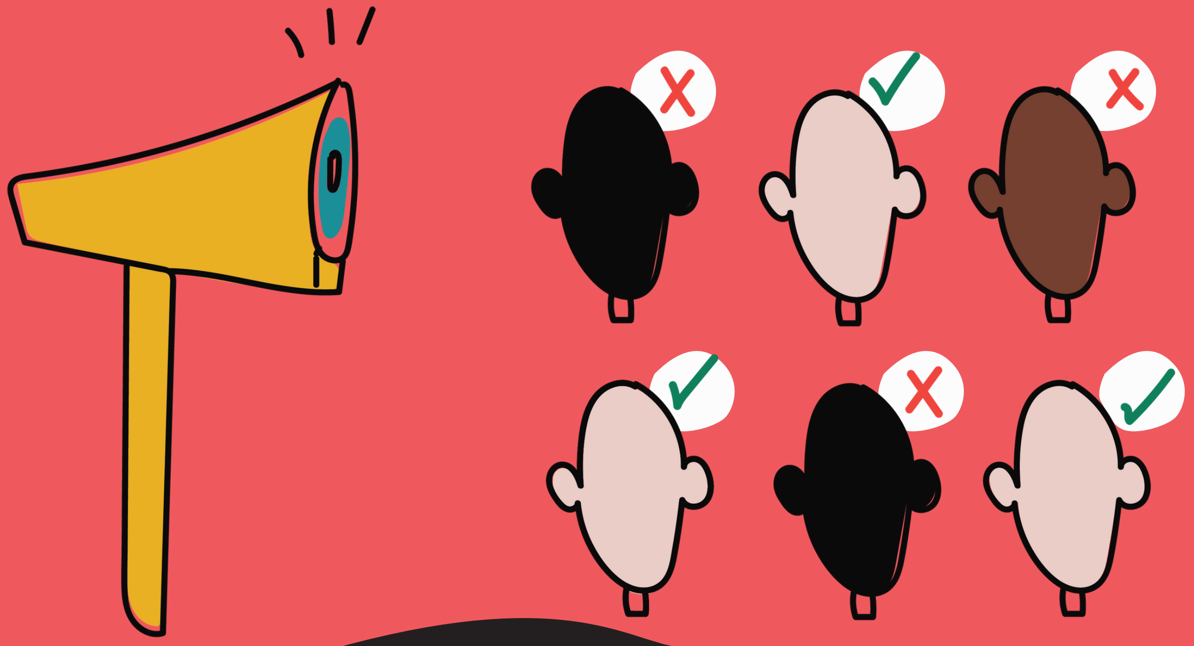
In a study by Pro Publica it was found that the software mislabeled black defendants as being twice as likely to be high risk of reoffending than white defendants- even though they didn't reoffend. White defendants on the other hand, were mislabeled at a low risk of reoffending- even though they did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

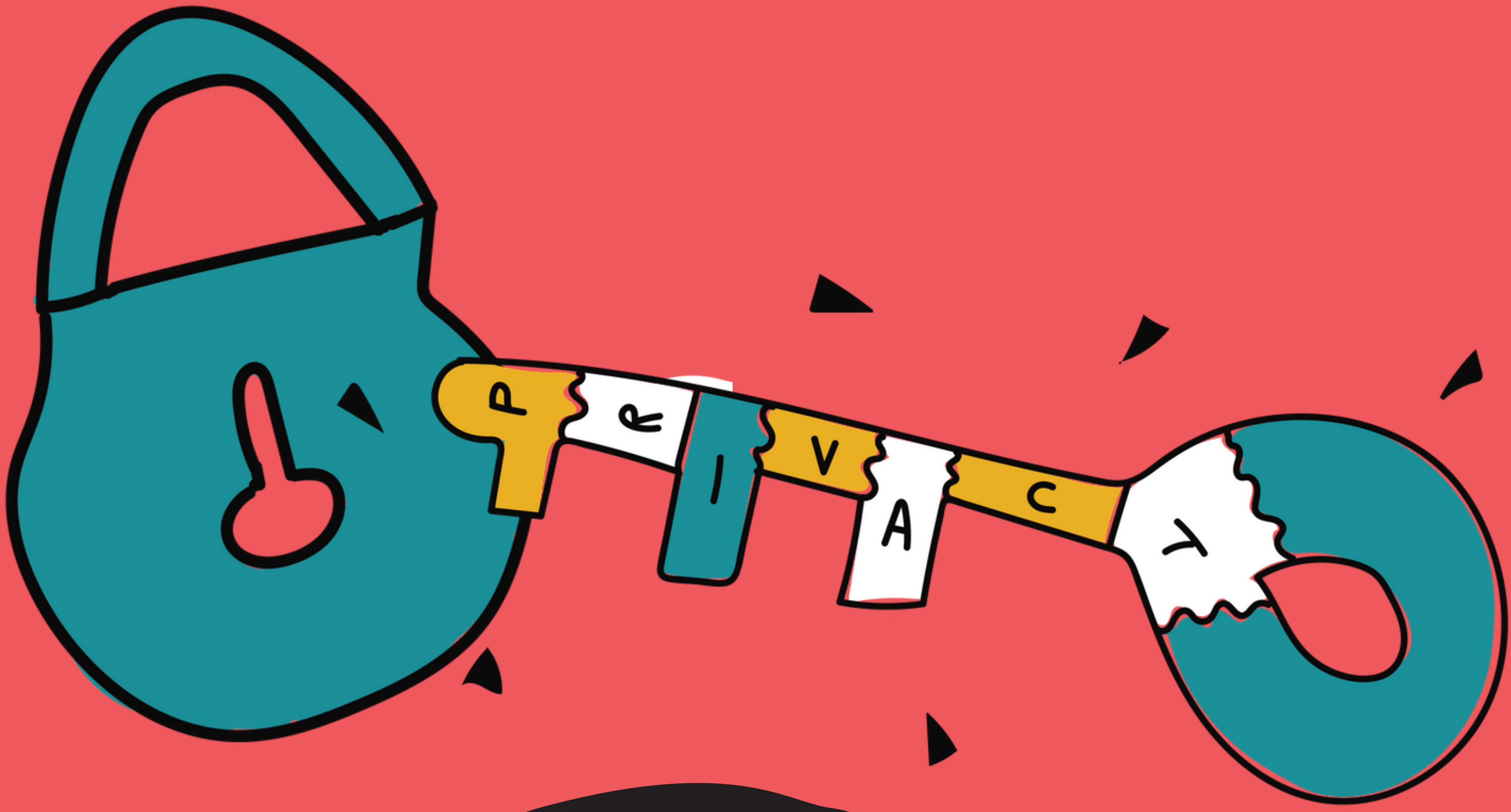
To put that into context, the data industry has now become more valuable than oil. Our data has become a seemingly unlimited resource to extract and profit from.

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.

Check out our Further Resources section for tips on stronger passwords.

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.

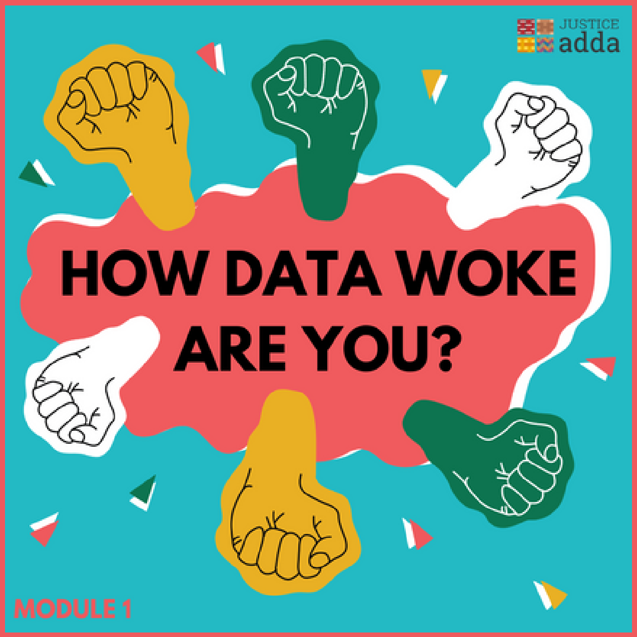
The point isn't that you shouldn't use your phone, that social media is a bad thing, or that you need to feel guilty about granting permissions to apps on your phone.

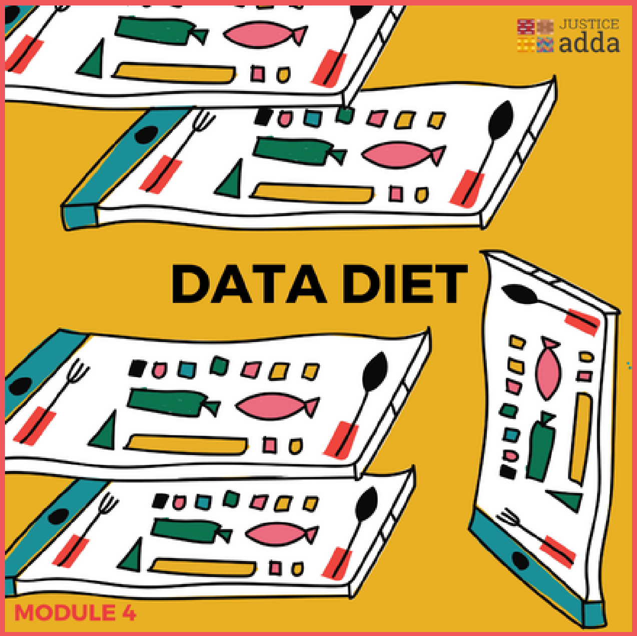
The point is that you need to be more informed about your data and how it can be used against you.

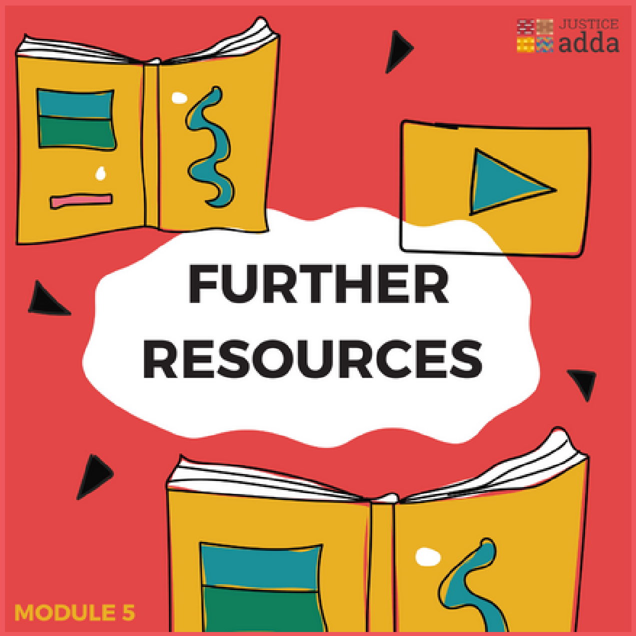
It is about creating awareness so that the next time an app asks you for a permission or your government asks you for data, you'll think twice and ask yourself, "Is this really necessary?"

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.

Also Check Out:







JUSTICE
adda

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