Privacy, Tracking & Your Digital Shadow

Cookies · App Permissions · Targeted Ads · Data Privacy

⏱ 55–65 min

GRADES 9–12

Previously in Chapter 1 – Aryan & Priya's Story

Aryan lost ₹14,000 from his family's UPI account because he reused one password everywhere. His sister Priya helped him fix it using Bitwarden and Gmail 2FA. They are now Cyber Safety Ambassadors at their school. In this chapter, Aryan discovers a **new and sneakier threat** — and a new friend, **Naman**, becomes the one who needs help this time!

📖 Chapter 2 – Privacy, Tracking & Your Digital Shadow

📰 Breaking Story – Read This First!

THE DIGITAL DISPATCH

Tuesday, 10th March 2026 · Privacy & Technology Edition

⚠ SPECIAL REPORT: HOW YOUR FREE APPS ARE TRACKING EVERY MOVE ⚠

🎯 DELHI STUDENT SEARCHED "CRICKET SHOES" ONCE — SAW ADS FOR 3 WEEKS ACROSS 7 DIFFERENT APPS

By Our Technology Correspondent, New Delhi

Naman, a Class 11 student from Rohini, Delhi, searched for cricket shoes on a popular e-commerce app last month. Within hours, he began seeing shoe advertisements on Instagram, YouTube, and even in a weather app. One week later, his mother — who uses the same Wi-Fi — started receiving shoe advertisements on *her* phone too.

"I felt like someone was watching me," said Naman. "I hadn't told anyone I was looking for shoes. How did my weather app know?" Investigation reveals Naman had accepted **"All Cookies"** on the e-commerce website, granted **location access** to many apps, and had **Ad Personalisation** turned on in his Google account — all without realising what these permissions actually meant.

How the data trail worked: The e-commerce site dropped a tracking cookie, which was shared with an advertising network. That network — connected to Instagram, YouTube, and thousands of other apps — served Naman targeted shoe ads across all platforms simultaneously.

The Wi-Fi connection: Because both phones shared the same IP address, the advertising network inferred a "household profile" and began targeting Naman's mother as well.

What experts say: "Students accept permissions and cookies without reading them. A single 'Accept All' click can authorise tracking across hundreds of websites for months."

⚠ **Every free app you use has a cost — your personal data. You are not the customer. You are the product.**

🤔 Stop & Reflect – Two Students, Two Views

After reading this story, two students in Aryan's class reacted very differently. Read both views below, then answer the question.

🧑 Riya's View

"I don't mind if apps track me. They just show me ads for things I already like. The service is free — it's a fair trade. I have nothing to hide."

🧑 Dev's View

"This is a privacy violation. I never agreed to have my data sold to unknown companies. The free service is not worth giving up control of my personal information and habits."

Your turn: **Whose view do you agree with more, and why? Is "free + tracked" always a fair trade? Write 2–3 sentences in your notebook.**

🔑 Key Terms

Cookie

A tiny file a website saves on your browser to **remember you** — your login, preferences, and what you clicked on.

App Permission

When an app asks to access your **camera, location, contacts,** or microphone. You can allow or deny each one.

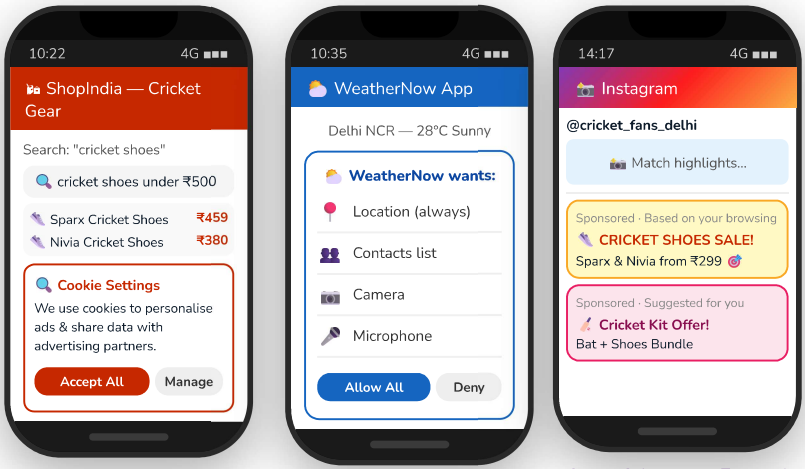
Targeted Ad

An ad **chosen for you** based on your browsing, location, and interests — tracked by cookies & apps.

Digital Footprint

Every trace you leave online — searches, posts, purchases, locations. **Never fully disappears.**

Real Screens — What Tracking Looks Like on Your Phone



Screen 1: "Accept All" Cookie Banner

Screen 2: Weather App 4 Unnecessary Permissions

Screen 3: Instagram Targeted Ads Based on His Search

Stop & Think — Before Moving On!
Screen 2's Weather App asks for **Contacts, Camera & Microphone** — a weather app only needs **location**. Those extra permissions build a richer data profile to sell to ad networks. **Convenience is what they offer. Your data is the price.**

Activity 1

Naman's Story — Comprehension & Analysis

Q1a.

What caused Naman's cricket shoe ads to appear on his mother's phone too?

- ○ His mother also searched for cricket shoes on her phone
- ○ Both phones shared the same home Wi-Fi IP address — advertisers inferred a household profile
- ○ Naman's mother had the same shopping app installed
- ○ Naman shared his browsing history with his mother via Bluetooth

Q1b.

Look at Screen 2 (WeatherNow). Tick: MAKE SENSE for a weather app, or RED FLAG?

Permission Requested	Makes Sense ✅	Red Flag 🚩	Why?
📍 Location (always on)	☐	☐	
👥 Access to Contacts	☐	☐	
📷 Camera	☐	☐	
🎤 Microphone	☐	☐	

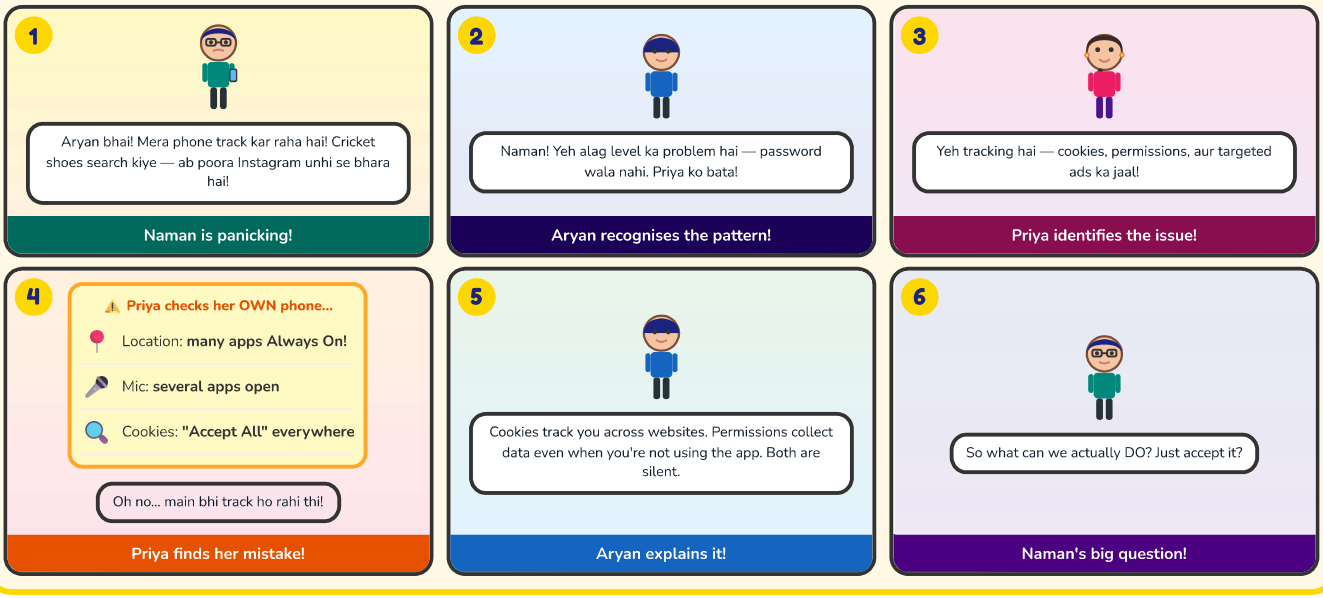
Q1c.

The news article says: *"You are not the customer. You are the product."* Explain what this means and give one example:

Story – "The Invisible Watcher": Naman Gets Help from Aryan & Priya

After seeing the news article, Naman reaches out to Aryan and Priya for help.

"Yaar, Koi Mujhe Dekh Raha Hai!" – Naman's Shock & Aryan's Revelation



Activity 2

Priya's Cookie Analysis – Help Identify the Risk

Let's assume Priya inspected her browser cookies on a study website. For each cookie, write whether Priya should keep or delete it.

#	Cookie Source	Type	What it does	Risk	Keep or Delete?
1	gmail.com	Session	Keeps Priya logged into her Gmail	LOW	
2	studysite.in	Persistent	Remembers her subject preferences for 1 year	MED	
3	doubleclick.net	Third-Party	Tracks her across many websites for ad targeting	HIGH	
4	facebook.com	Third-Party	Tracks her even on sites she's never visited with her Facebook account	HIGH	
5	youtube.com	Persistent	Remembers watch history and preferences for 2 years		

Q2a.

Why is the doubleclick.net cookie more dangerous than the gmail.com session cookie, even though both are linked to Google?

Q2b.

Priya asks: "If I delete all cookies, I'll lose my logins — so what's the point?" Is she correct? What is the smarter approach?

🎯 How Targeted Ads Work — The Profile They Build About You

📊 What Companies Know About a Typical Class 11 Student (Naman's Data Profile)

Let's assume this is what a data profile for a student like Naman might look like — built silently from his apps and browsing.

Location	Interests	Inferred Income	Behaviour Patterns
Rohini, Delhi	Cricket, gaming	Middle-class	Active 4–10pm
School: 9am–3pm	Budget shopping	Searches under ₹500	Buys after 3 views
Home: rest of day	Bollywood music	Family of 4	Responds to discounts

⚠ **This profile was built without Naman ever filling out a single form.**
All of this was inferred from cookies, location permissions, search history, and ad click behaviour — automatically, silently, and continuously.

😱 Story Twist — Priya's Shocking Discovery!

💬 "Priya's Social Media Experiment" — One Week Later

Priya: Aryan, I did an experiment! I mentioned "new shoes" once near my phone — without searching anything — and next morning I saw shoe ads on Instagram!

Aryan: It's more likely your search history and location patterns were enough. Companies don't even need to listen — they already know enough to predict what you'll want next!

Naman: So they know me better than I know myself? They can predict what I'll want next even before I search it?

Priya: Exactly! That's called **profiling.** The real danger is not just ads — this data can be used to manipulate your opinions, emotions, and decisions.

📊 Why This Matters — Tracking in India

📊 Let's Assume — What the Data Might Look Like for Students in India

These are illustrative figures to help you think about the scale of tracking — not attributions to any specific source.

~8 in 10	₹1000s Cr	~7 in 10	4+ hrs
free Android apps request at least one unnecessary permission unrelated to the app's core function	estimated value of Indian users' personal data bought and sold annually by data brokers	teenagers click "Accept All" on cookie banners without reading what they are agreeing to	average daily screen time for Indian teens — generating enormous amounts of behavioural data

Q. Look at the "~8 in 10 apps" figure. Why do you think so many free apps ask for permissions they don't need? What is their real motivation?

Q. The average Indian teen spends 4+ hours on screen daily. What does this mean for the amount of data being collected about them? Give one specific example of what a company could infer from this.

Activity 3

🔍 App Permission Audit — Help Naman Fix His Phone!

Let's assume Naman found these permissions on his Android phone (Settings → Apps → Permissions). For each row, tick whether the permission MAKES SENSE or is a RED FLAG, rate the risk, and write what Naman should do.

App	Permission Granted	Makes Sense ✅	Red Flag 🚩	Risk Level	What should Naman do?
🔦 Flashlight App	📍 Location (always on) 👥 Contacts access	☐	☐		
📷 Camera App	📷 Camera 🖼 Photo Gallery	☐	☐		
🎮 Free Cricket Game	🎤 Microphone (always on) 📍 Location (always on) 👥 Contacts	☐	☐		
🗺 Google Maps	📍 Location (while using app)	☐	☐		
🌤 Weather App	📍 Location (always on) 🎤 Microphone 👥 Contacts 📷 Camera	☐	☐		
📞 WhatsApp	🎤 Microphone 📷 Camera 👥 Contacts 🖼 Gallery	☐	☐		

Q3a.

The Free Cricket Game is asking for Microphone (always on) and Location (always on). Suggest TWO possible reasons WHY a game developer might want these permissions that have nothing to do with the game itself:

Q3b.

Priya makes a rule: *"Location should be set to 'While Using App' — never 'Always On'"* for all apps except navigation. Explain why "Always On" is more dangerous than "While Using App" for location access:

Activity 4

⚖️ Situation Analysis — What Would You Do?

Read each situation. Decide if the person's action is SAFE ✅ or RISKY ⚠️. Then write what they should do and why.

Situation 1 — Aarav's Free Game App

Let's assume Aarav (Class 10) downloads a free IPL cricket game. During install, it asks for: Location (always on), Microphone, Contacts, and Camera. He clicks "Allow All" because the game looks fun and it's free.

Safe ✅ or Risky ⚠️? ☐

Name TWO specific risks. What should Aarav do instead?

Situation 2 — Meera's Cookie Choice

Let's assume Meera (Class 12) visits a news website. A cookie banner appears with three options: "Accept All", "Reject All", "Manage Preferences". She clicks "Manage Preferences", turns off third-party and tracking cookies, but keeps functional cookies. The site loads slightly slower.

Safe ✅ or Risky ⚠️? ☐

What did Meera do RIGHT? Was the trade-off worth it?

🛡️ Priya's 5-Step Privacy Action Plan — Do These on Your Own Phone!

📋 Priya's Privacy Checklist — Can You Complete These Right Now?

1. **🔍 Audit Your App Permissions (Android: Settings → Apps → Permissions)**
   For every app: Is location set to "Always"? Turn it to "While Using App" or "Off". Remove Camera/Mic from any app that doesn't genuinely need it (torch, calculator, alarm, weather).
2. **🔍 Stop Clicking "Accept All" on Cookie Banners**
   Always click "Manage Preferences". Turn OFF: "Third-party cookies", "Tracking cookies", "Advertising cookies". Keep only: "Functional" and "Necessary" cookies.
3. **🎯 Turn Off Ad Personalisation on Google**
   Go to: myaccount.google.com → Data & Privacy → Ad Settings → Turn off "Personalised Ads". Also do this in your Facebook/Instagram settings under "Ad Preferences."
4. **🌐 Use a Privacy-Focused Browser for Sensitive Searches**
   Use Firefox or Brave browser for searches. These block third-party trackers by default. Use "Incognito/Private" mode when you don't want searches saved to your device.
5. **📱 Review App List Every 3 Months — Delete What You Don't Use**
   Every app you keep = ongoing data collection, even when you're not using it. Unused apps with microphone or location access continue collecting data in the background.

Activity 5

🎮 Privacy Habit Sort — Smart or Risky?

Aryan listed 8 digital habits from a class discussion. Sort each numbered habit into the correct zone. Then answer the questions.

Habits to sort:

1. Clicks "Accept All" cookies on every website
2. Location set to "While Using App" for Maps only
3. Downloads free games and grants all permissions
4. Reviews cookie preferences & rejects third-party
5. Has many unused apps still installed on his phone
6. Turns off Ad Personalisation in Google settings
7. Uses a free VPN with "no logs" claim from unknown developer
8. Uses Firefox browser with privacy mode for sensitive searches

✅ SMART Privacy Habits

Write habit numbers here...

⚠️ RISKY Privacy Habits

Write habit numbers here...

Q4a.
Habit 7 mentions a "free VPN from an unknown developer." Explain why a poorly chosen VPN can actually be *worse* for your privacy than having no VPN at all:

Q4b.
Naman says: "I'll just delete all social media and stop using the internet." What does he gain? What does he lose? What is a more realistic and balanced approach?

🧠 Deep Analysis — Apply What You've Learned

Challenge Activity

🔬 Two Complex Scenarios — Think It Through

📋 Scenario A — "The Free Period Tracker App"

Let's assume Tanvi, a Class 12 student, uses a popular free period tracking app. She logged her menstrual dates, mood, and symptoms for a year. She later discovers that the app's privacy policy allowed it to share this "anonymised" health data with third-party "research partners" — which could include insurance companies. Tanvi had clicked "I Agree" on a long Terms of Service without reading it.

CA1.

Identify TWO privacy problems in this scenario. For each, explain: (a) what data was exposed, and (b) what potential harm could result:

Problem 1:

Problem 2:

CA2.

The app's developer argues: "All data sharing was disclosed in our Terms of Service. Users agreed." Is this a morally acceptable defence? Give arguments for both sides, then state your own judgement:

Developer's argument:

Counter-argument:

My judgement:

📋 Scenario B — "The Persuasion Machine"

Let's assume a food delivery platform has analysed Naman's data profile: he orders most on rainy evenings, always chooses ₹50-or-below delivery, and is most likely to impulse-order when watching cricket. The platform now: (1) sends push notifications during India matches; (2) shows expensive combo meals first — knowing he'll scroll to cheaper ones anyway; (3) automatically enables "Express Delivery" (₹30 extra), requiring him to actively deselect it. Naman notices he's spending significantly more per month than he intends to.

CB1.

The platform uses THREE specific manipulation techniques based on Naman's data. Identify each and explain how his data was used to design it:

Technique 1:

Technique 2:

Technique 3:

CB2.

Design your own "Personal Digital Privacy Policy" — a set of rules you will personally follow online. Cover: (a) permissions, (b) cookies, (c) targeted ads, (d) what data you will and won't share. Write at least 5 specific rules:

🎨 Creative Challenge — Be the Privacy Advocate!

Activity 6

📢 Design a "Privacy Awareness" Campaign for Your School!

You, Aryan, Priya, and Naman are launching a school campaign: *"Check Before You Click."* Design one of the campaign materials below. Your material must cover: what cookies/permissions are, why they matter, and one actionable step students can take today.

🎨 Option A: Campaign Poster

🔍 CHECK BEFORE YOU CLICK!

What are cookies? (Draw/write)	Permission Red Flag (Draw/write)
1 Action for Today (Write)	Your Privacy Slogan (Write)

📱 Option B: Instagram Story Script (3 slides)

Design 3 story slides: Slide 1 = Hook, Slide 2 = Explain the problem, Slide 3 = What to do. Each slide max 15 words + emoji.

Slide 1 (Hook):

Slide 2 (Problem):

Slide 3 (Action):

🌟 Epilogue — Three Months Later: Naman Teaches His Class

3 Months Later	Campaign Impact	Aryan's Growth	The Real Lesson ✅
Naman: "I used to click 'Accept All' without thinking. Now I know that one click can fund an entire advertising profile about me."	**Priya:** "We taught fellow students how to manage cookie settings and ran a permission audit — many students had unnecessary permissions on their phones!"	**Aryan:** "After Chapter 1 fixed my passwords, Chapter 2 made me realise — security and privacy are both needed. You need both layers."	**All Three:** "Convenience and privacy are a trade-off. We can't avoid all tracking — but informed choices make us harder to exploit."

🌟 Key Takeaways

📱 Permissions Have a Purpose — Check Them
Every permission you grant is a data collection channel. Only allow what the app genuinely needs. Location = "While Using App" — never "Always On".

🔍 Never Click "Accept All" on Cookies
Third-party cookies track you across the entire internet for months. Always choose "Manage Preferences" and reject tracking and advertising cookies.

🎯 Targeted Ads Use Your Data Profile
Companies build a detailed model of your personality and habits — without you filling out a single form. Turn off Ad Personalisation in Google and Meta settings.

⚖️ Privacy is a Trade-off — Make Informed Choices
Every free service has a data cost. Informed decisions — reading permissions, rejecting unnecessary cookies — make you significantly harder to exploit.

🏆 Aryan, Priya & Naman's Golden Rule

"Check permissions before installing. Choose 'Manage' over 'Accept All'. Turn off Ad Personalisation. Ask: what am I giving up for this free service?"

Because in the digital world, if you're not paying for the product — you ARE the product.