YIGF CAMBODIA 2026

Your Data, Your Safety

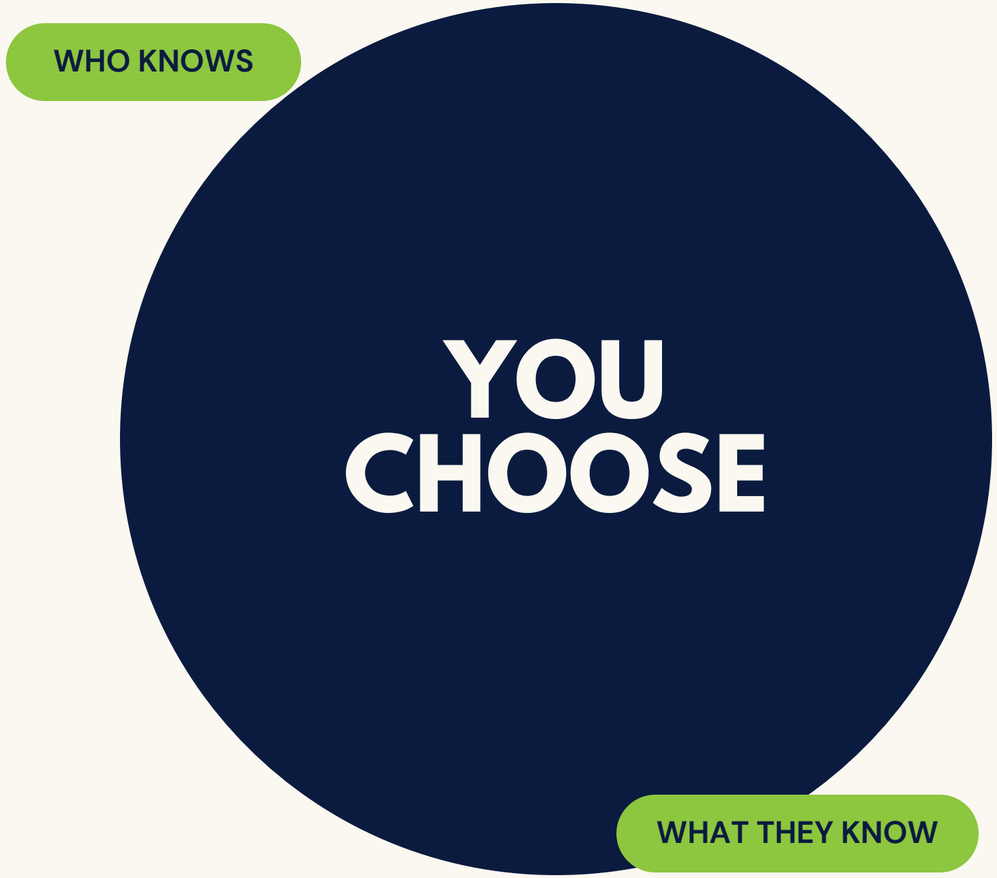
Empowering Cambodian Youth to Protect Their Personal Information Online

By: Jenn Bunny
Founder of The Blueprint



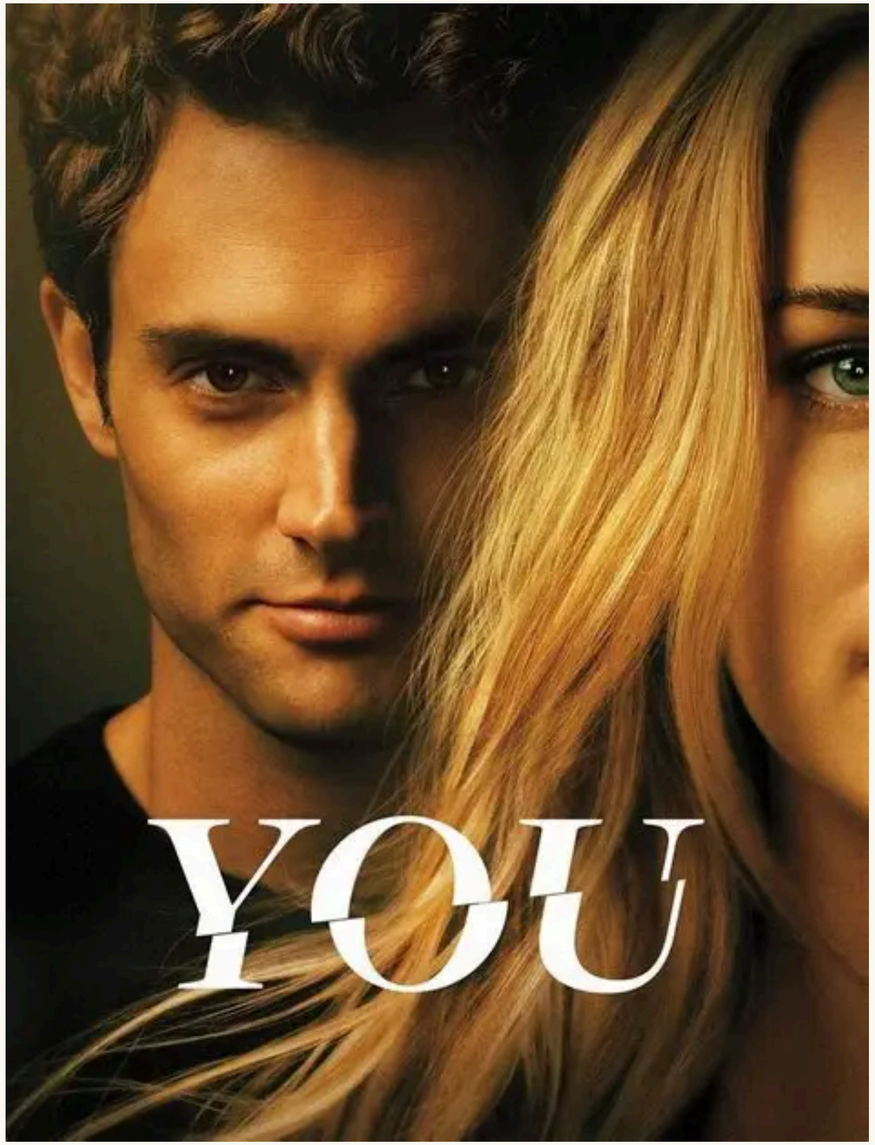
I have nothing to hide

Privacy is not secrecy.



How many people used real name on their Facebook account?

Have anyone watched YOU movie before?




clideo.com

What counts as personal data?

Any information that can point to you, on its own or when combined with other details.

WHAT COUNTS AS DATA

Who you are: name, face, ID number

How to reach you: phone, email, address

Where you are: live location, saved places

What you do: searches, likes, purchases

What you use: device ID, contacts, messages

If it can be linked back to you, it is your data.

If I never share my name, can anyone still find me?

What makes it identifiable?

Small details that look harmless can still point to one person.

- Age: 19
- Studies at: RUPP university
- Lives in: Santhormuk area
- Rides home: 9pm every day
- Orders food: Friday nights

TOGETHER THEY SHOW

ONE PERSON

A 19 year old student at RUPP university, living in Santhormuk area, riding home at 9pm every day. Easy to find, easy to follow, easy to target.

The danger is not one detail. It is the combination.

How your data gets misused

Four common ways it happens online.



Phishing

Fake links and messages that trick you into giving your login.

PROTECT YOURSELF

Check the sender. Do not tap unknown links.



Scams

Fake prizes, jobs or loans that ask for money or your OTP code.

PROTECT YOURSELF

Never share your OTP. Verify on official pages.



Impersonation

Fake accounts using your name and photos to fool your friends.

PROTECT YOURSELF

Lock your profile. Report fake accounts.



Doxxing

Your address, phone or workplace posted online to harass you.

PROTECT YOURSELF

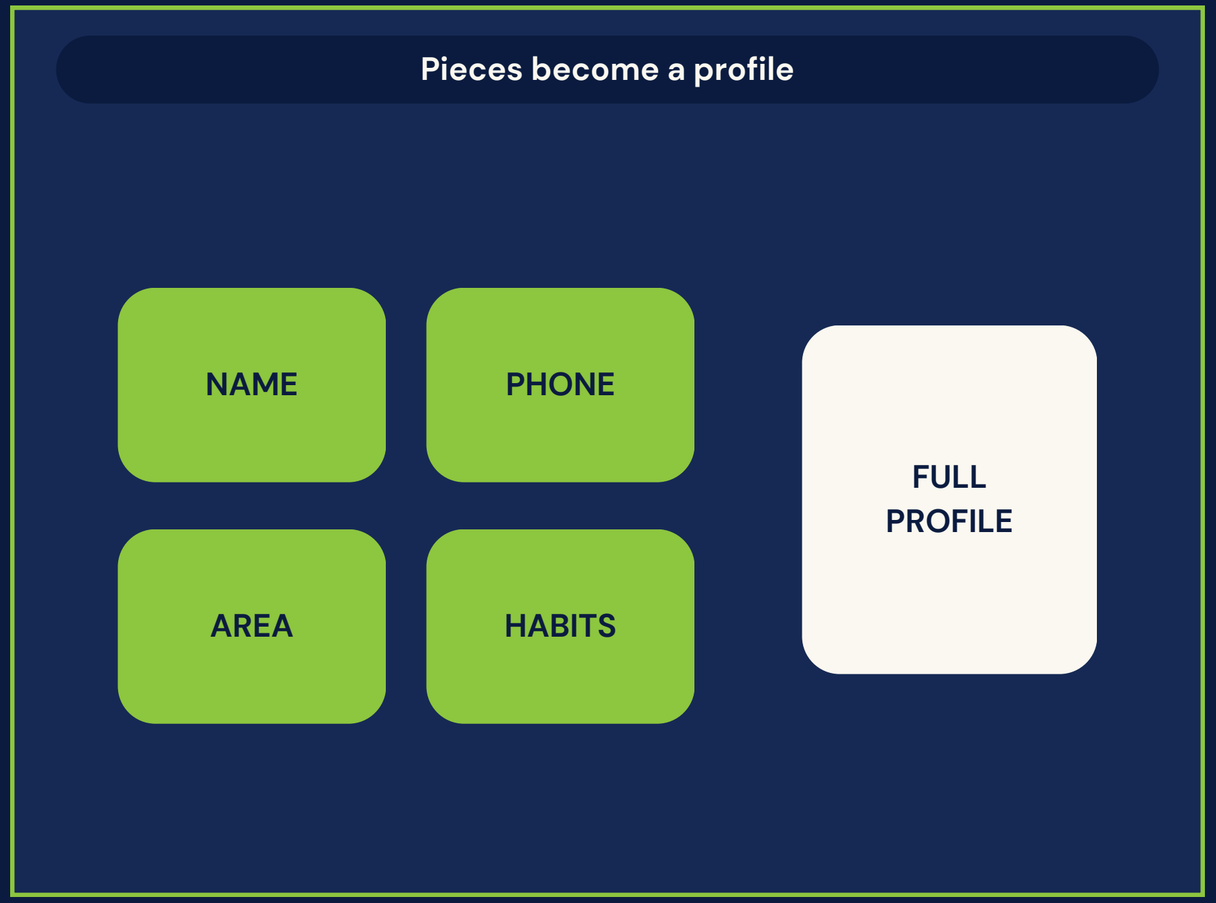
Limit public details. Avoid tagging your location.

Most attacks begin with one small piece of data you shared.

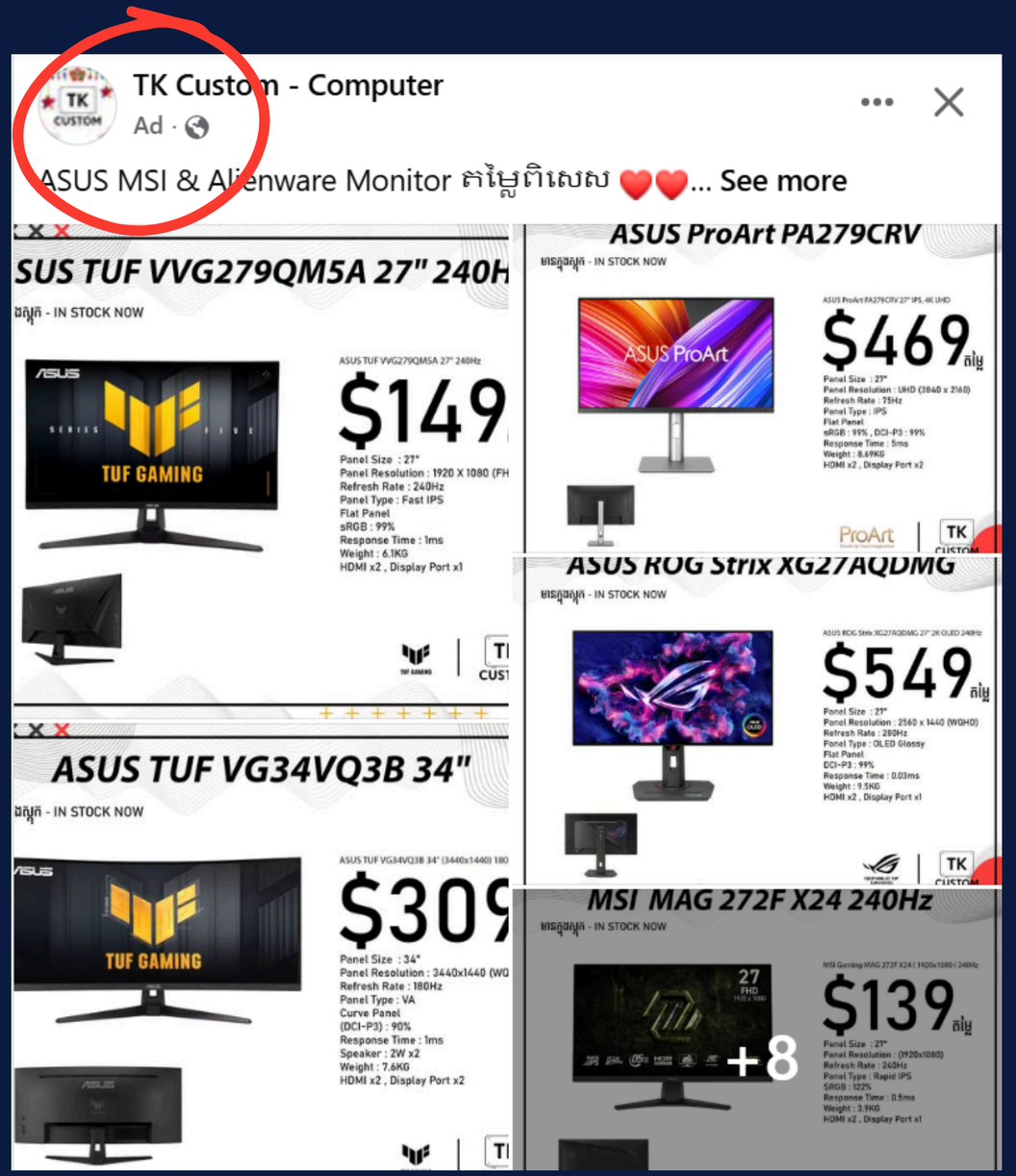
There’s no free breakfast

When an app costs nothing, your data is often the payment. Small pieces combine into a detailed picture of you.

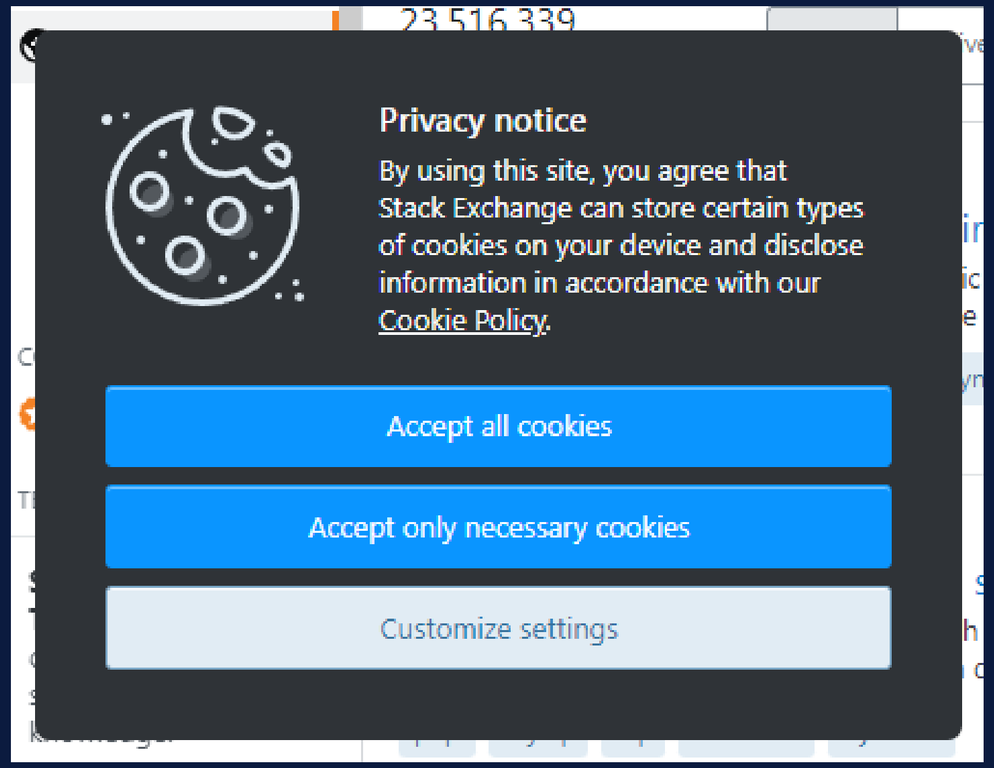
- **One app knows your name**
- **Another knows your number**
- **Together they know your habits**

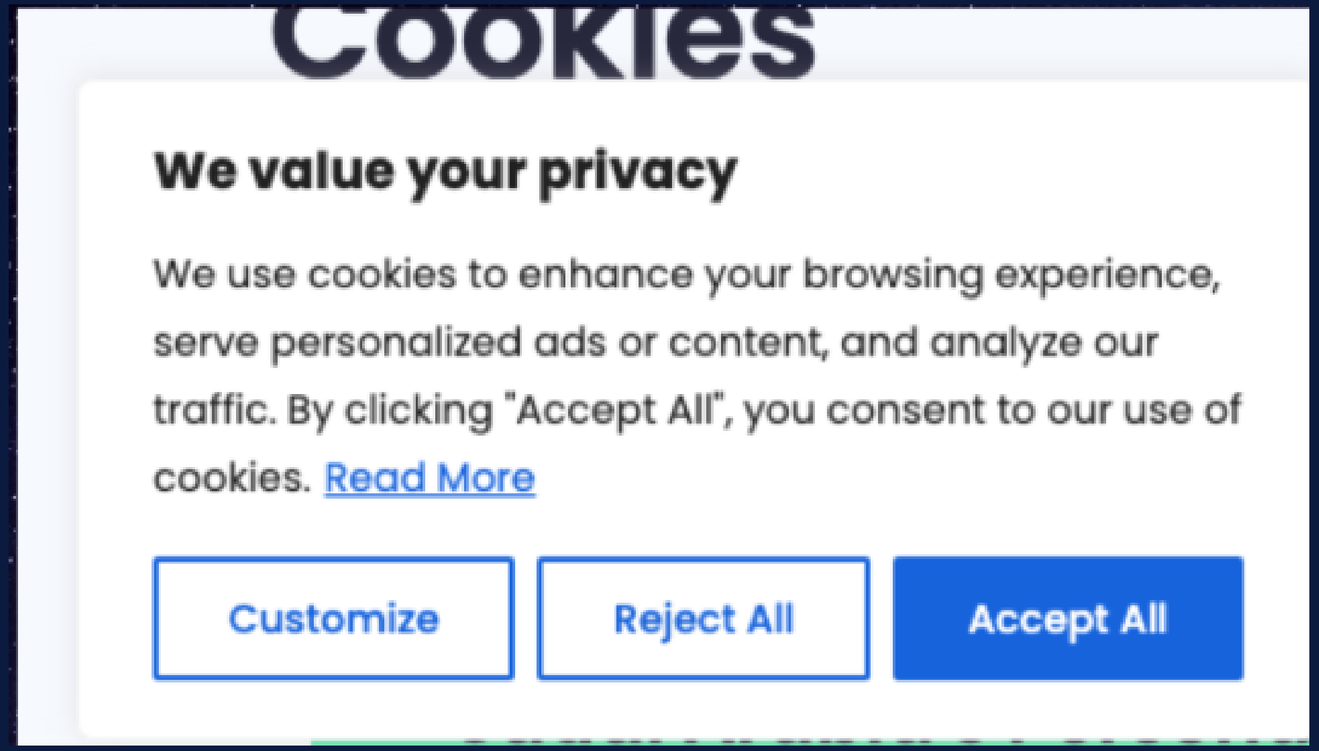


How do they know I wanted to buy a monitor?



Tracking


23,516,339
Privacy notice
By using this site, you agree that Stack Exchange can store certain types of cookies on your device and disclose information in accordance with our Cookie Policy.
Accept all cookies
Accept only necessary cookies
Customize settings


Cookies
We value your privacy
We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept All", you consent to our use of cookies. Read More
Customize
Reject All
Accept All

Case: Target, 2012



Forbes

Subscribe: Less than $2/wk

TECH

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

By Kashmir Hill, Former Staff. Welcome to The Not-So Private Parts where technology & privacy collide

Published Feb 16, 2012, 11:02am EST, Updated Aug 11, 2022, 04:17am EDT

Source: The New York Times and Forbes, 2012.

Case: Target, 2012

A store worked out a teenager's pregnancy before her family knew.

1. The data

Target gave shoppers a pregnancy prediction score, based on buying habits like unscented lotion, vitamins and large bags of cotton balls.

2. The prediction

The score flagged a teenage girl as likely pregnant. She never told Target. Her shopping data did.

3. The leak

Maternity coupons were mailed to her home. Her father opened them and found out before she had told him.

THE LESSON

Everyday purchases can reveal private facts.

No one asked her. She never shared it. The data did the telling, and it told her family first.

Source: The New York Times and Forbes, 2012.

Be careful what you tell AI

Chatbots feel private. They are not always.

It can be stored

Your chats may be saved by the company and read by staff or reviewers.

It can train AI

Some tools learn from what you type, unless you opt out.

It can leak

Breaches, shared chat links and mistakes can expose your words.

DO NOT PASTE INTO AI

- ID, passport or bank details
- Passwords and OTP codes
- Private photos of you or others
- School, work or client secrets
- Health or family problems
- Anything you would not post publicly

Simple rule: if you would not post it publicly, do not paste it into AI.

Why should you care about your digital footprint?

Anyone can look you up.



- It lasts. Screenshots keep what you delete.
- It travels. Anyone can search your name.
- It gets judged. Often without context.

Two real situations

VISA

Officials may read your accounts

Some applicants must make their profiles public.

70%

JOBS

of employers search you online

Over half found a reason not to hire.

Sources: US State Department visa screening updates, 2026. CareerBuilder employer survey.

Who protects your rights?

Everyone has a role.

Government

Pass clear laws and set up an independent data authority.

Companies

Collect less data, explain it clearly and keep it secure.

Schools, media

Teach digital skills and raise awareness in the community.

You and friends

Use privacy settings, report misuse and help friends do the same.

Clear laws, responsible companies and informed people work together.

Your data privacy rights

Most data protection laws around the world give you these six rights.

Be informed

Know what data is collected and why.

Access

See the data a company holds about you.

Correct

Fix data that is wrong or out of date.

Delete

Ask a company to remove your data.

Object

Say no to certain uses, or take back your consent.

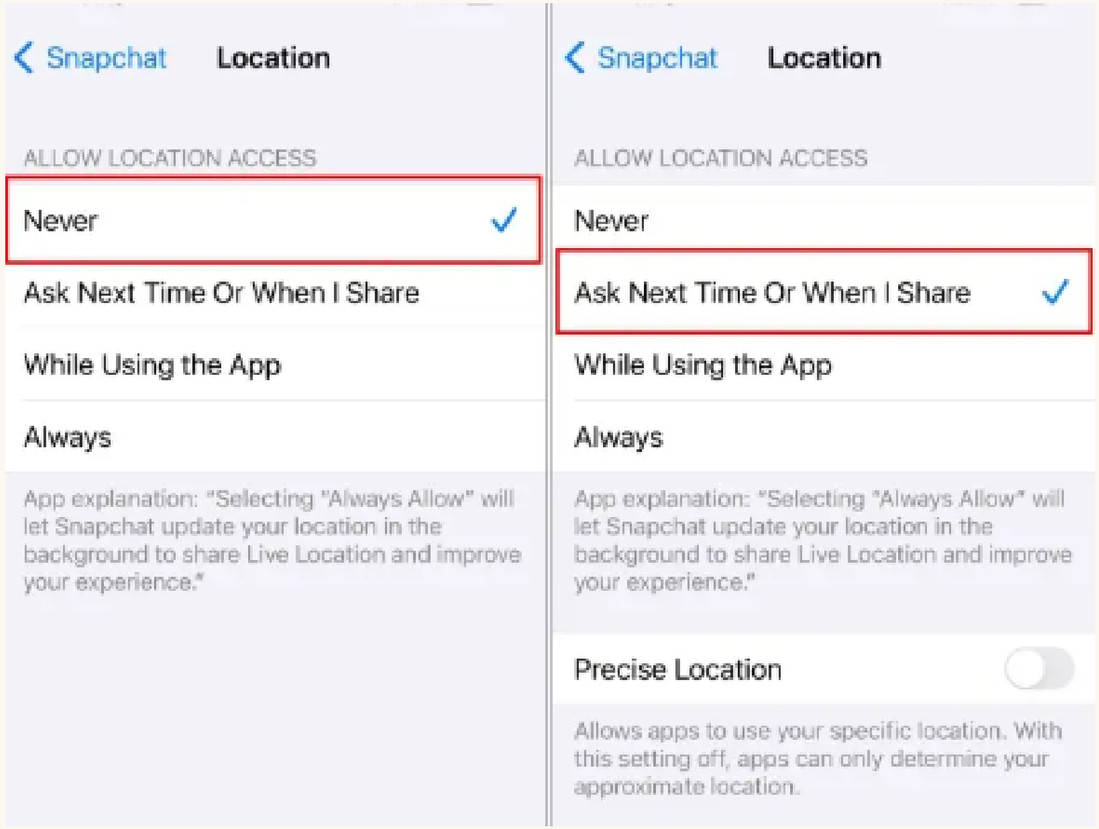
Complain

Report misuse to the data protection authority.

Cambodia is still drafting its personal data protection law. Know these rights and ask for them.

Tips to protect your data

1. **Turn off location when you can**
   Settings, then Location. Set it to off or while using.
2. **Use a fake name or email**
   For sign ups that do not need your real identity.
3. **Use in app chat for delivery**
   Keep your real phone number from drivers and riders.
4. **Use a unique password**
   One password per account, so one leak stays small.
5. **Turn on two step verification**
   Even if someone has your password, they cannot log in.
6. **Clear cookies often**
   Accept necessary cookies only. Cookies track your habits.
7. **Review permissions and privacy settings**
   Delete saved addresses and limit what each app can see.



Thank you

Reachable via bunnysereivathna@gmail.com