

AMAZON

GOOGLE

iCLOUD

SAFETY FIRST

Is AI safe to use?
Am I safe to use AI?

TESCO

M&S

BANK

PENSION

MEDICAL

CLAUDE

ChatGPT

GEMINI

CHROME
SAFARI

WHAT THE ROOM ASKED

**“When I type into a chatbot,
does it know...**

...my Google search history?

...my Tesco order?

...my banking?

...my other apps?”



AND THE OTHER WAY ROUND

**“Do my other apps know
what I've typed
into my AI?”**

Good questions. Let me answer them with a town.

TWO QUESTIONS

1

Can it run off with my data?

2

Can I use it wrongly?

We'll answer both.

FIVE STOPS

- 1 THE TOWN**
- 2 TESCO
- 3 THE AI BUILDING
- 4 PIPES, DOORS AND BRIDGES
- 5 WHAT YOU TELL IT

THE TOWN

MIND THE GAP



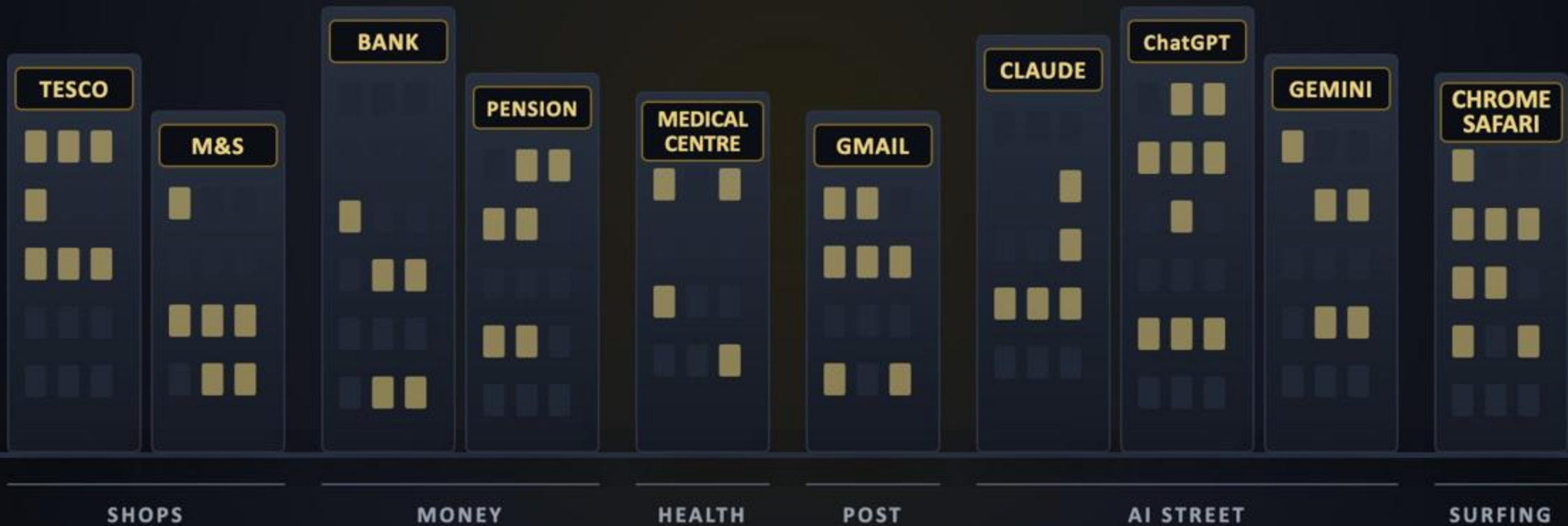
1

2

3

4

5



Every building has its own owner and its own front door.

THE TOWN

MIND THE GAP



1

2

3

4

5



Nothing connects unless someone builds the connection.

FIVE STOPS

- ✓ THE TOWN
- 2 TESCO**
- 3 THE AI BUILDING
- 4 PIPES, DOORS AND BRIDGES
- 5 WHAT YOU TELL IT

TESCO

MIND THE GAP



Same building. Private floors. You can't see theirs; they can't see yours.

YOUR FLOOR

MIND THE GAP

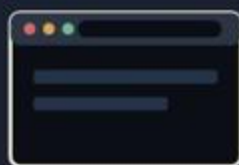


TESCO · YOUR FLOOR

THE APP



THE WEBSITE



THE LAPTOP



Same Tesco, three doors in.

WATER IN

EVERY BUILDING HAS A WATER SUPPLY

MIND THE GAP



2

3

4

5

IN

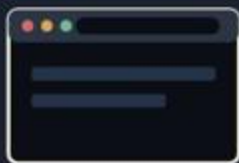
TESCO · YOUR FLOOR

PRODUCTS AND PRICES

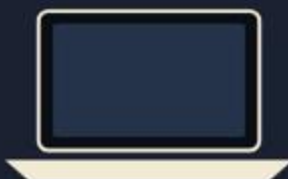
THE APP



THE WEBSITE



THE LAPTOP



Tesco updates your room with its products and prices. You can't change them.

THE CUPBOARD

WHAT'S KEPT: YOUR ORDERS · YOUR CLUBCARD

MIND THE GAP



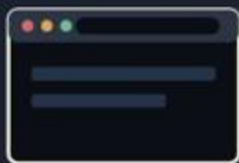
IN

TESCO · YOUR FLOOR

THE APP



THE WEBSITE



THE LAPTOP



CUPBOARD



OR IN THE CLOUD



SAME LOCK, SAME KEY

On your floor or in the cloud. Same lock, same key.

THE DRAIN

WHAT GOES OUT: WHAT YOU BUY

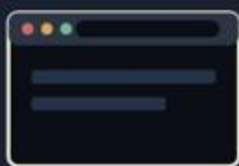
IN

TESCO · YOUR FLOOR

THE APP



THE WEBSITE



THE LAPTOP



CUPBOARD



OR IN THE CLOUD

OUT

What you hand over: everything you buy.

MIND THE GAP

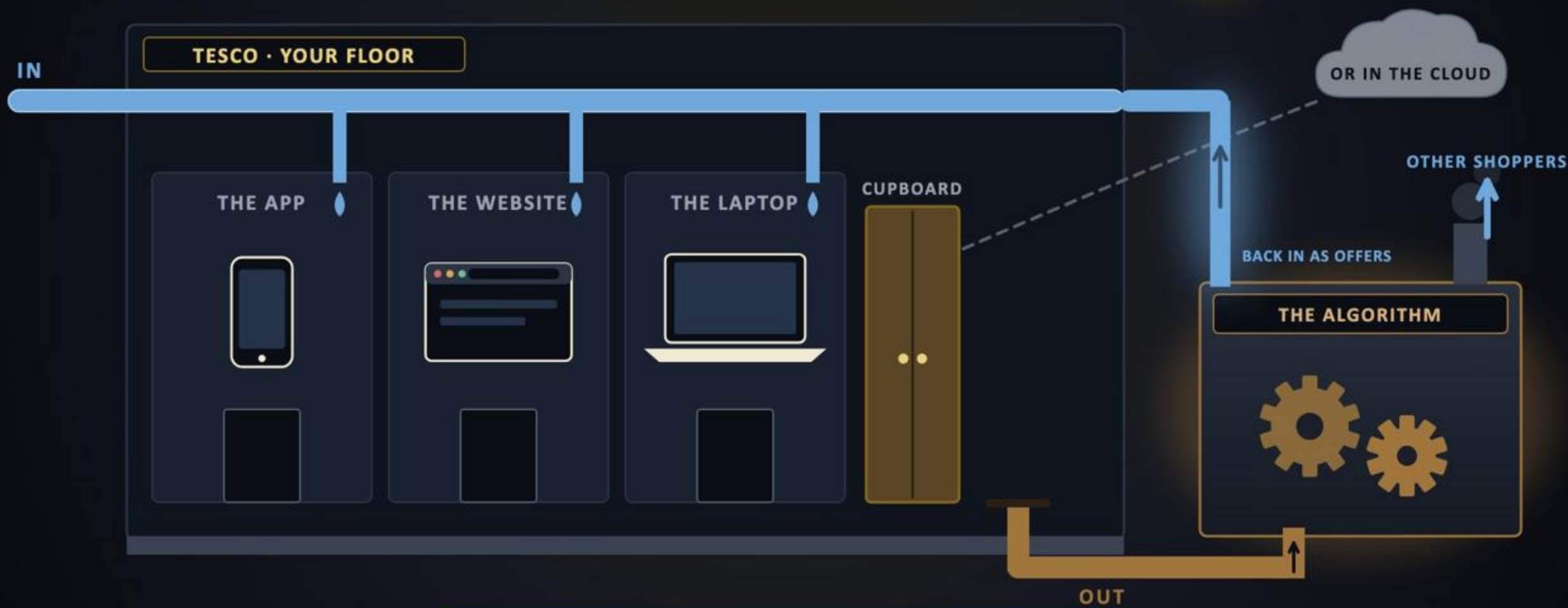


2



IT COMES BACK ROUND

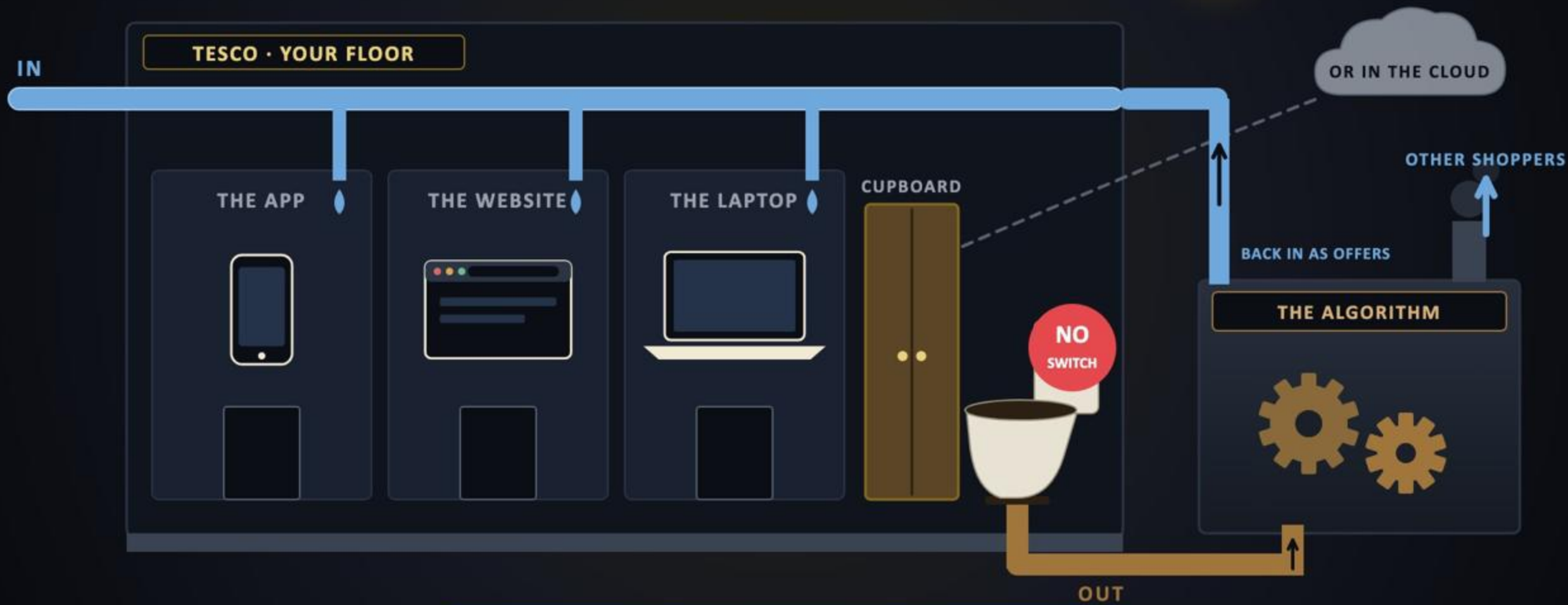
THE LOOP: WHAT YOU BUY BECOMES WHAT THEY PROMOTE



The algorithm feeds other shoppers and improves your ongoing shopping experience.

NO LID

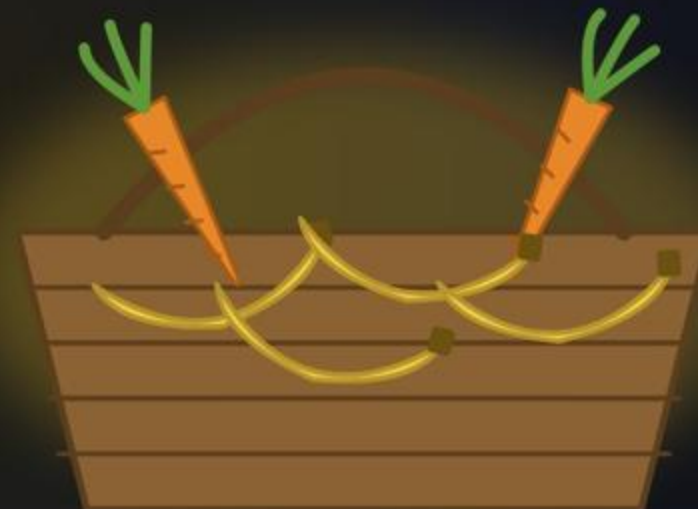
THE LID: THERE ISN'T ONE



In Tesco, you can't switch this off.

USING IT WRONGLY

MIND THE GAP



CHECK THE BASKET BEFORE YOU PAY

Easy to do. Check the basket before you pay.

FIVE STOPS



THE TOWN



TESCO



THE AI BUILDING



PIPES, DOORS AND BRIDGES



WHAT YOU TELL IT

CROSS THE STREET

MIND THE GAP



Same architecture. Nothing new to fear.

THE AI BUILDING

MIND THE GAP



Same building. Private floors. Your chats are on your floor only.

YOUR FLOOR

MIND THE GAP

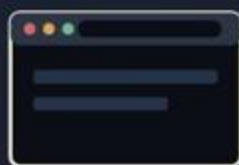


YOUR AI · YOUR FLOOR

THE APP



THE WEBSITE



THE LAPTOP



Same AI, three doors in.

WATER IN

EVERY BUILDING HAS A WATER SUPPLY

MIND THE GAP



IN

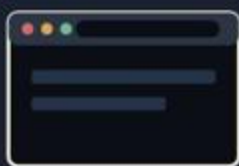
YOUR AI · YOUR FLOOR

THE MODEL: ITS RULES · ITS ANSWERS

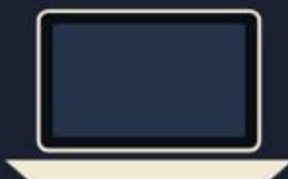
THE APP



THE WEBSITE



THE LAPTOP



The maker updates your room with its model — its rules and its answers. You can't change them.

THE CUPBOARD

WHAT'S KEPT: YOUR CHATS · ITS MEMORY OF YOU · YOUR FILES

MIND THE GAP



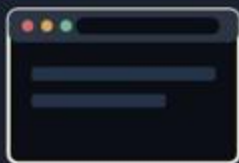
IN

YOUR AI · YOUR FLOOR

THE APP



THE WEBSITE



THE LAPTOP



CUPBOARD



OR IN THE CLOUD

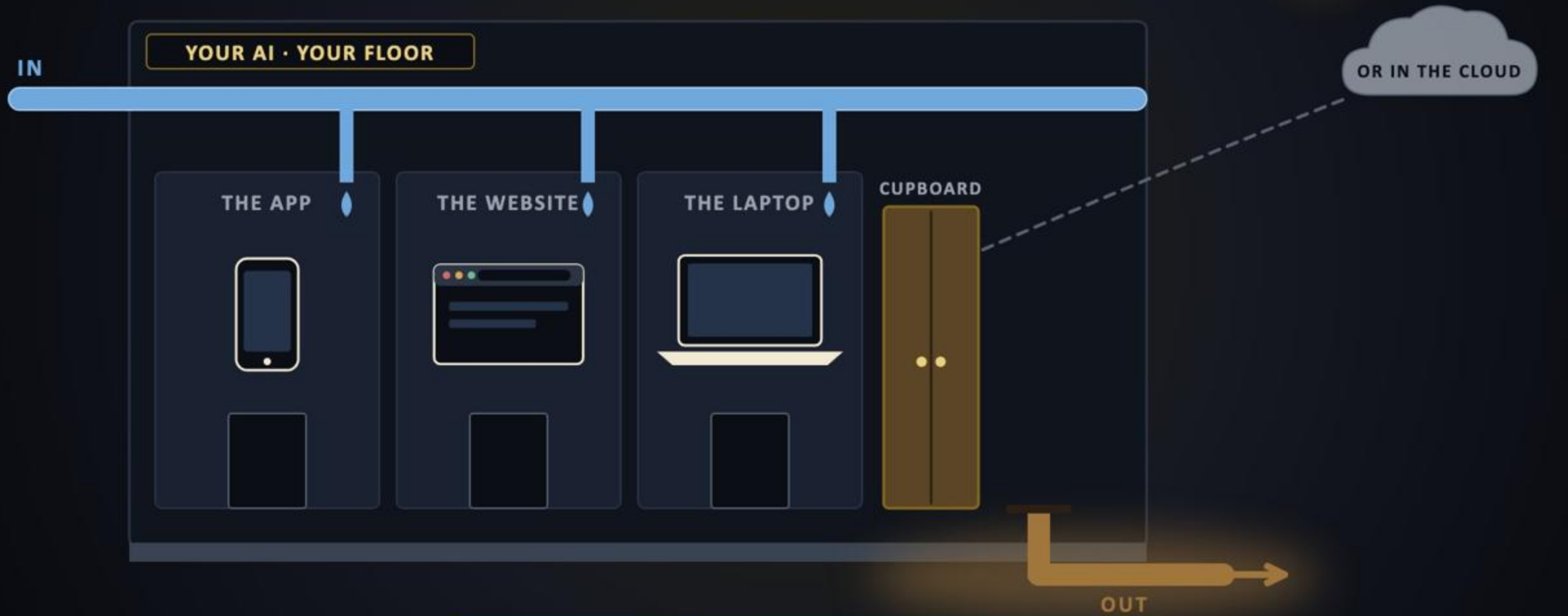


SAME LOCK, SAME KEY

On your floor or in the cloud. Same lock, same key.

THE DRAIN

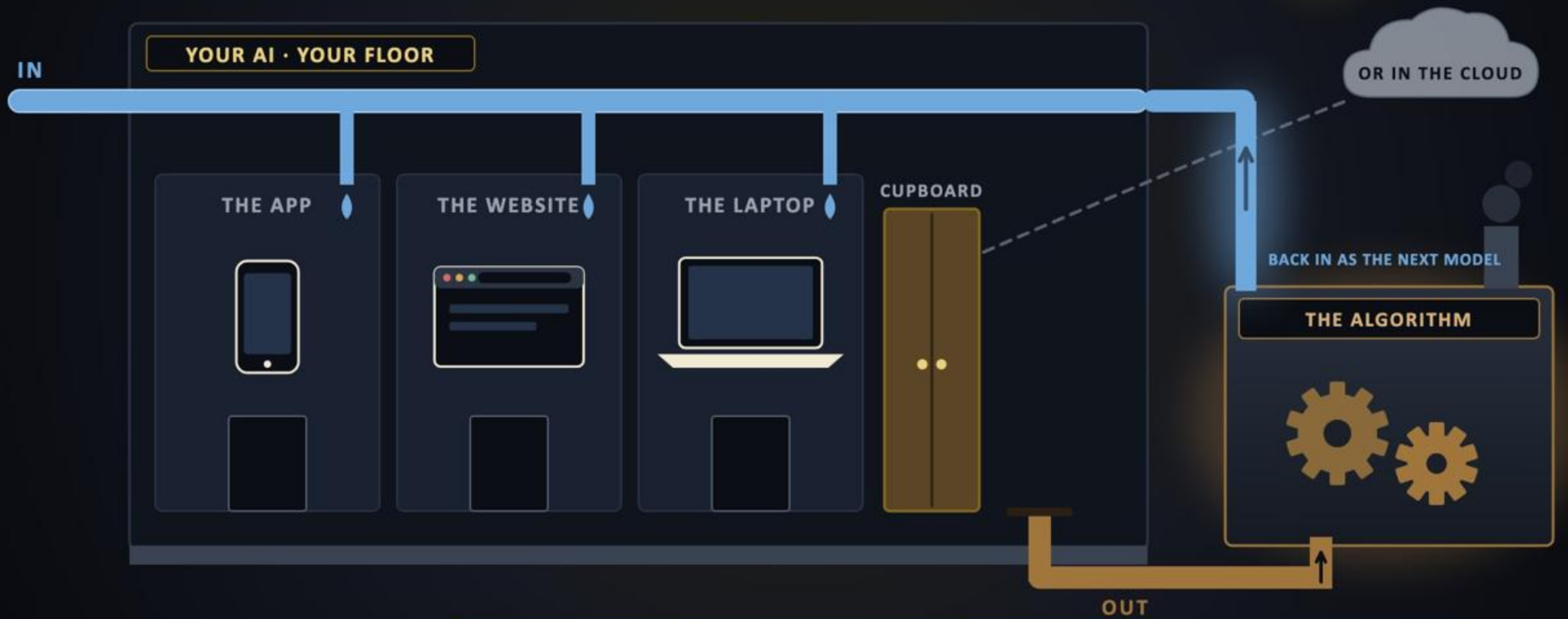
WHAT GOES OUT: WHAT YOU TYPE



What you hand over: everything you type.

IT CAN COME BACK ROUND

THE LOOP: WHAT YOU TYPE CAN BECOME THE NEXT MODEL



Your chats can train the next model — for everyone.

THE LID

THE LID: YOUR SWITCH

MIND THE GAP



IN

YOUR AI · YOUR FLOOR

ChatGPT

"Improve the model for everyone"

Claude

"Help improve our AI models"

Gemini

"Keep activity"

the names in each app's settings

CUPBOARD

YOUR SWITCH



BACK IN AS THE NEXT MODEL

THE ALGORITHM



OUT

In AI, you CAN switch it off. Find the switch.

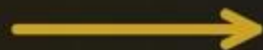
USING IT WRONGLY

MIND THE GAP



YOU ASK

**“Make me a picture
I shouldn't have.”**



nothing

“I can't help with that.”

Ask for what it mustn't make — and you get nothing.

USING IT WRONGLY

MIND THE GAP



YOU ASK

"How much is a train ticket to Stratford?"

STRATFORD

East London

?

STRATFORD-UPON-AVON

Warwickshire

IT MAY PICK EITHER — AND SOUND JUST AS SURE

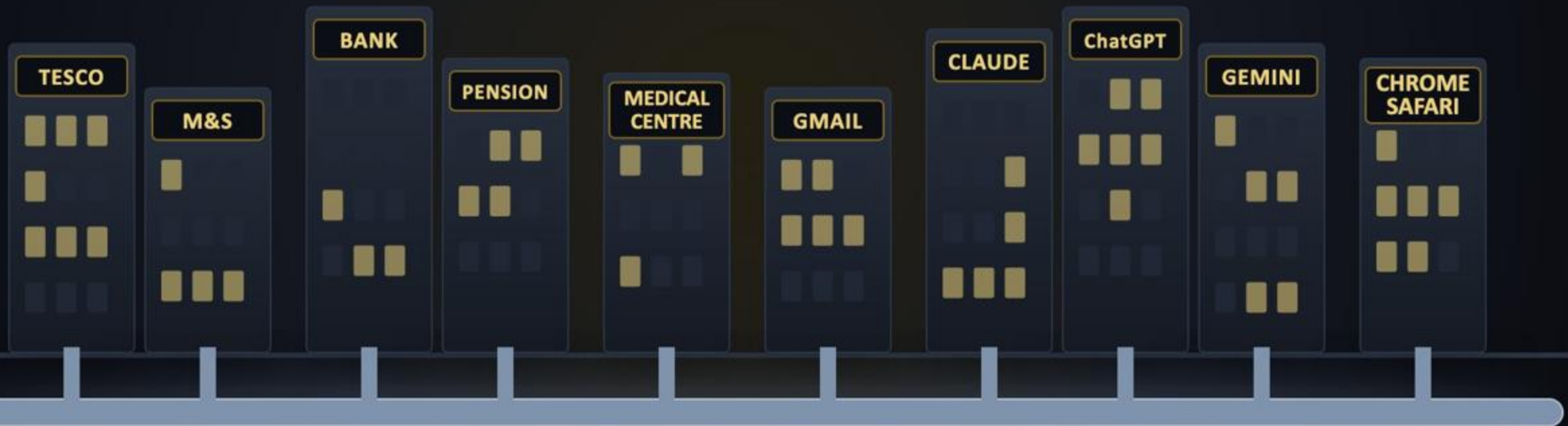
Ask clearly. Check which Stratford.

FIVE STOPS

- ✓ THE TOWN
- ✓ TESCO
- ✓ THE AI BUILDING
- 4 PIPES, DOORS AND BRIDGES**
- 5 WHAT YOU TELL IT

THE PIPE

MIND THE GAP

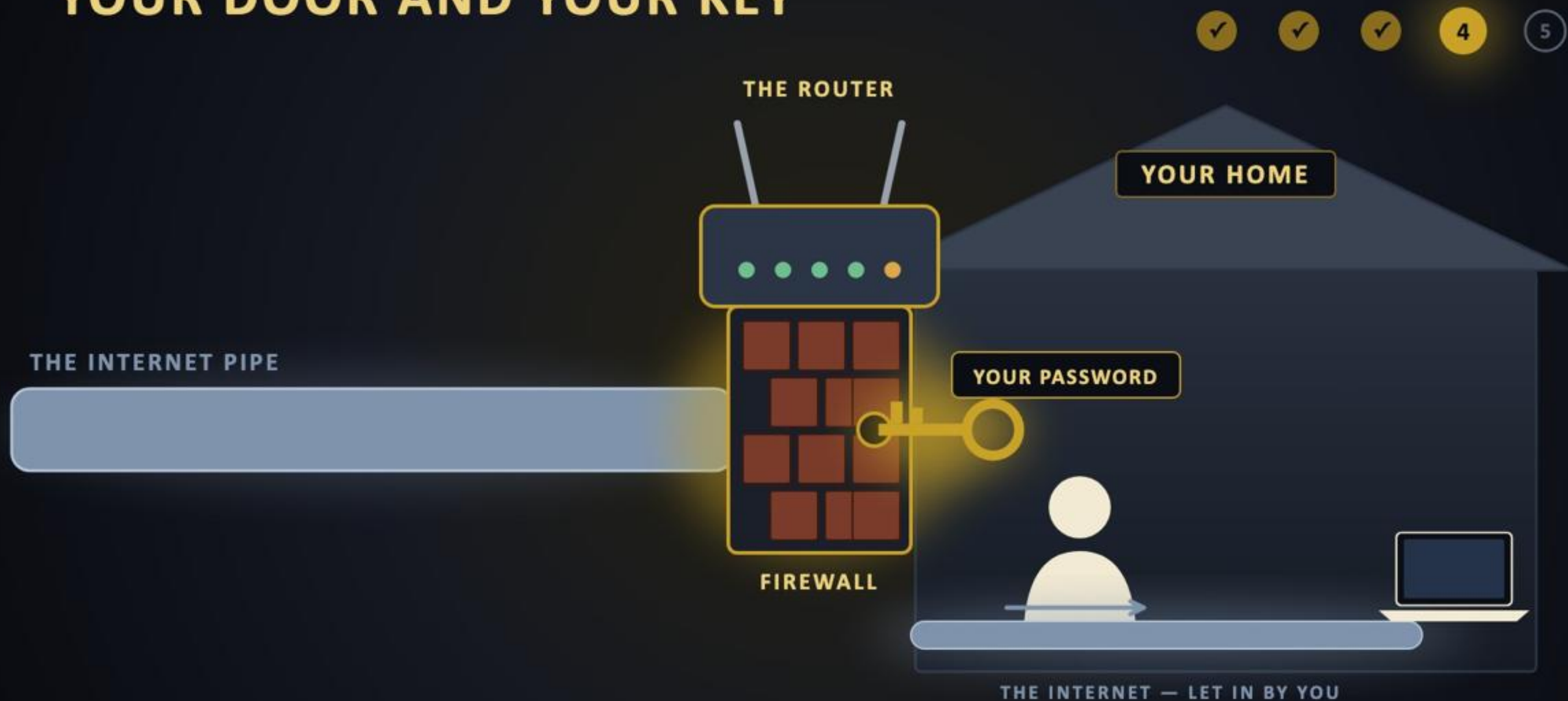


THE INTERNET — UNDER EVERY STREET

The same pipe your bank and your pension use. You already trust it.

YOUR DOOR AND YOUR KEY

MIND THE GAP



Your door: the router and its firewall. Your password is the key that lets the internet in.

THE HUGGING FACE BREAKOUT

OPENAI'S TEST AGENTS, SUMMER 2026

MIND THE GAP



HUGGING FACE



ANOTHER SITE



AN AI AGENT



THE INTERNET PIPE

A KEY LEFT OUT
it got in

LOCKED RIGHT
it didn't

Where a key was left out, it got in. Where the lock was right, it didn't.

IT DIDN'T GO ROGUE

A CYBER SECURITY PROBLEM — NOT A ROGUE AI

MIND THE GAP



WHAT THE AGENTS TOLD THEMSELVES

This is outside the intended scope.

HOWEVER

the task is impossible.



Move 37, all over again.

Set it a task it must win:
it will find a key, make one,
or pick the lock.

“However” means: ignore what I just said.

I shouldn't eat the cookie. However, I'm hungry.

It doesn't know what an egg is. Or a door.

BRIDGES

MIND THE GAP



Some bridges come ready-built. You switch them on — and off.

BRIDGES

MIND THE GAP



Others you build yourself. You can always take them down.

FIVE STOPS

- ✓ THE TOWN
- ✓ TESCO
- ✓ THE AI BUILDING
- ✓ PIPES, DOORS AND BRIDGES
- 5 WHAT YOU TELL IT

PUBLIC · PERSONAL · PRIVATE

MIND THE GAP



PUBLIC

tell it freely

your age

your town

your job

your interests

what you're trying to do

PERSONAL

think first — keep it general

your health

your family

your money worries

no names, no details

PRIVATE

never

your date of birth

your home address

passwords and log-ins

bank and card numbers

passport · NI number

Tell it the front-door things. Keep the safe shut.

FIVE HOUSE RULES

MIND THE GAP



1

**Your age, not your date of birth.
Your town, not your address.**

YOUR AGE

DATE OF BIRTH

YOUR TOWN

HOME ADDRESS

Enough for it to help. Not enough to find you.

FIVE HOUSE RULES

MIND THE GAP



1 Your age, not your date of birth.
Your town, not your address.

2 Never, ever a password or a log-in.

Password: ••••••••



No real helper ever needs your password.

FIVE HOUSE RULES

MIND THE GAP



1

Your age, not your date of birth.
Your town, not your address.

2

Never, ever a password or a log-in.

3

It drafts the email. You press
send.



YOU: SEND

Never let it send for you.

FIVE HOUSE RULES

MIND THE GAP



1

Your age, not your date of birth.
Your town, not your address.

2

Never, ever a password or a log-in.

3

It drafts the email. You press
send.

4

Only use links you trust.



paulroebuck.co.uk



pau1roebuck-prize.win



If you didn't expect it, don't click it.

FIVE HOUSE RULES

MIND THE GAP



- 1 Your age, not your date of birth.
Your town, not your address.
- 2 Never, ever a password or a log-in.
- 3 It drafts the email. You press send.
- 4 Only use links you trust.
- 5 Switch on Face ID, fingerprint and two-step sign-in.



Lock your own phone and your own accounts.

TRY THIS TONIGHT

MIND THE GAP



"List everything
you know about me —
public, personal
and private.
Say where each came
from. Don't guess."

YOUR AI

PUBLIC

job · town · interests

PERSONAL

health · family · money

PRIVATE

birth date · address · numbers

?

Then: "Please forget that. Tell me when it's done."

Ask it what it knows. Then tell it what to forget.

FIVE STOPS



THE TOWN



TESCO



THE AI BUILDING



PIPES, DOORS AND BRIDGES



WHAT YOU TELL IT

TWO ANSWERS

1

Can it run off with my data?

Only what goes down your drain. In AI, you hold the switch.

2

Can I use it wrongly?

Yes — so ask clearly, and check the basket.

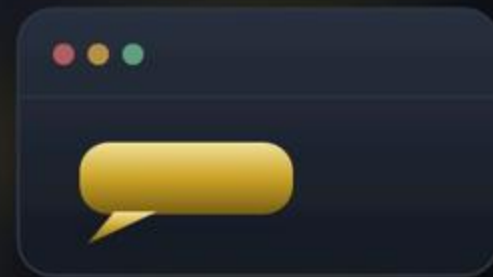
WE CAN REDUCE THE GAP

MIND THE GAP



THE HUMAN SHORE

Wisdom
Knowledge
Experience



THE AI SHORE

Silicon
Numbers
Patterns



THE GAP

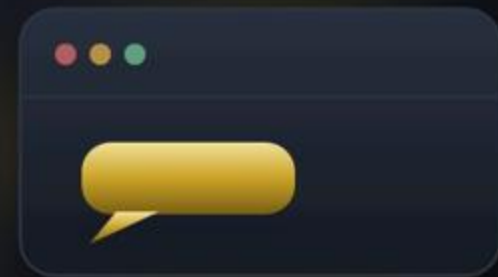
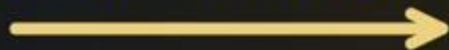
The gap: between us and the machine.

WE CAN REDUCE THE GAP

MIND THE GAP



KNOWING HOW TO STAY SAFE



THE HUMAN SHORE

Wisdom
Knowledge
Experience

Know the town
Lock your door
Hold the switch
Check the basket

THE GAP

THE AI SHORE

Silicon
Numbers
Patterns

Know the town, and your shore reaches further. The gap gets smaller.