CyPurr Session: Mobile Security

Can’t live with it, can’t live without it, want to throw it Over a bridge yeah…I understand

Cypurr Collective, May 15th 2021, Expiration: 11/2021

Overview

Intro

Mobile Security

Outro

Q/A

WHO ARE WE?

We are...

To educate the public on cybersecurity in an accessible and hollistic way with fun cats.

Our work aims to resist systemic oppressions through community self-defense.

We do that with programs, events, workshops, socials and more!

Established April 2016

GROUNDRULES

Saf(er) Space - We **DO NOT** tolerate language or behavior purposefully meant to demean or harm folks based on their identities

Webinar Mode- Send your questions through the chat, we'll try our best to answer them through the chat, on video, or during the Q/A, depending on what's going on.

WHO ARE WE?

Slides/Resources available after!
Video available soon.

A note on voice recording…

We are trying to keep these presentations for posterity, and not to record participants. **Use the chat if possible for questions and discussions if you do not want your voice on the recording.**

And now…

Cypurr Presents
Mobile Security

CyPurr Collective

First, some terms to keep in mind

Code: Instructions for your computer to complete.

"Open Source": A program that lets you read the instructions it contains (and even change them)

Proprietary: A program that keeps their instructions a secret

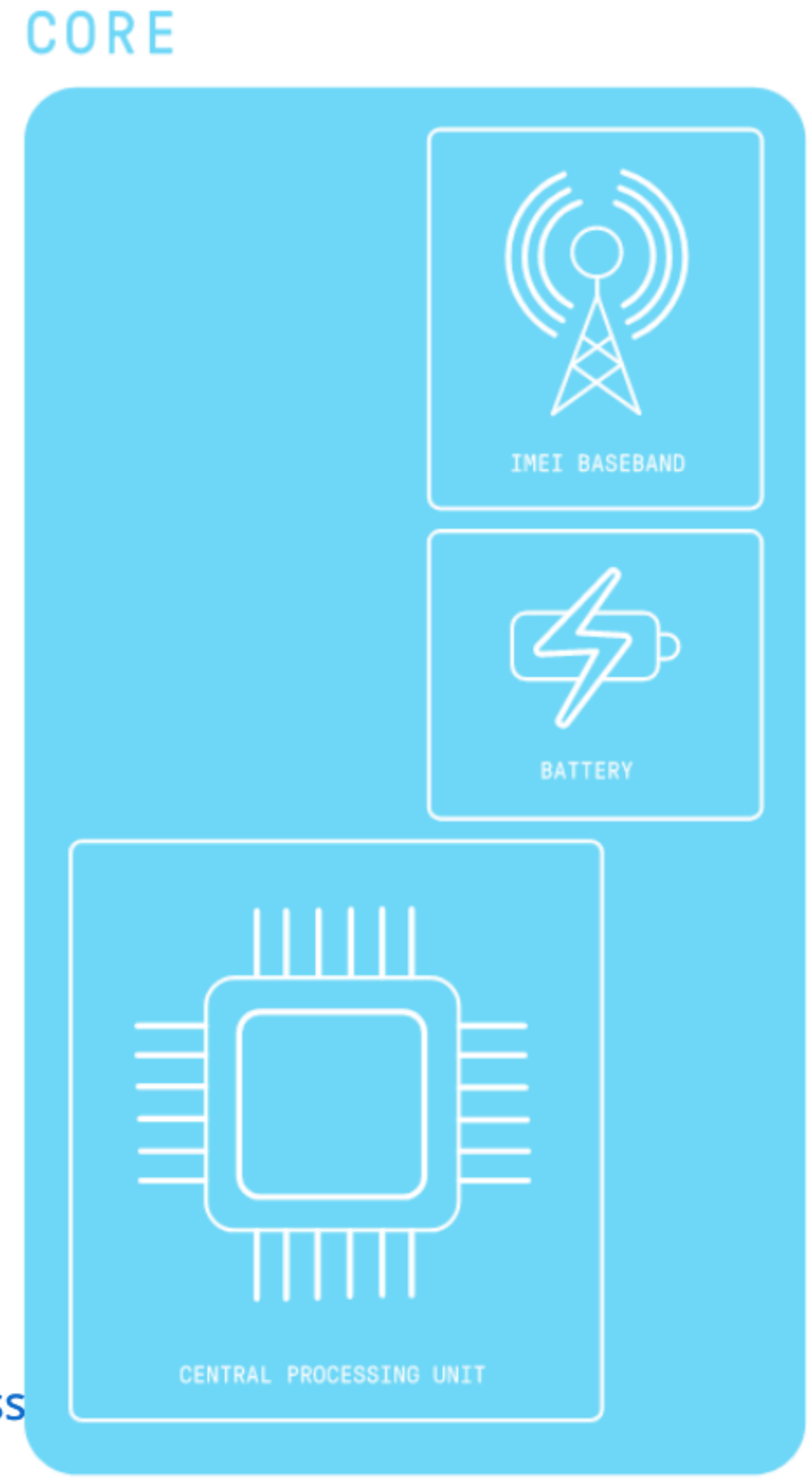
The Problem with Mobile Phones

- Not designed for privacy and security
- More locked down with ***proprietary*** code, making it harder to control than regular computers.
  - Can't change OS
  - Planned obsolescence with updates
  - harder to investigate malware
  - harder to prevent snooping
- Phones and Phone #s attached to our identity, finances, etc

More at ssd.eff.org

Building a smart phone

- Central Processing Unit (CPU)- Completes instructions from code
- IMEI- unique ID assigned to every phone
- Baseband Processor (bbp)- Manages all radio functioning
- The bbp acts as a second mind, running its own ***proprietary code***



Images from MyShadow.org & Tactical Tech Collective Glass Room

"Smart" Components

SD card- "Secure Digital"

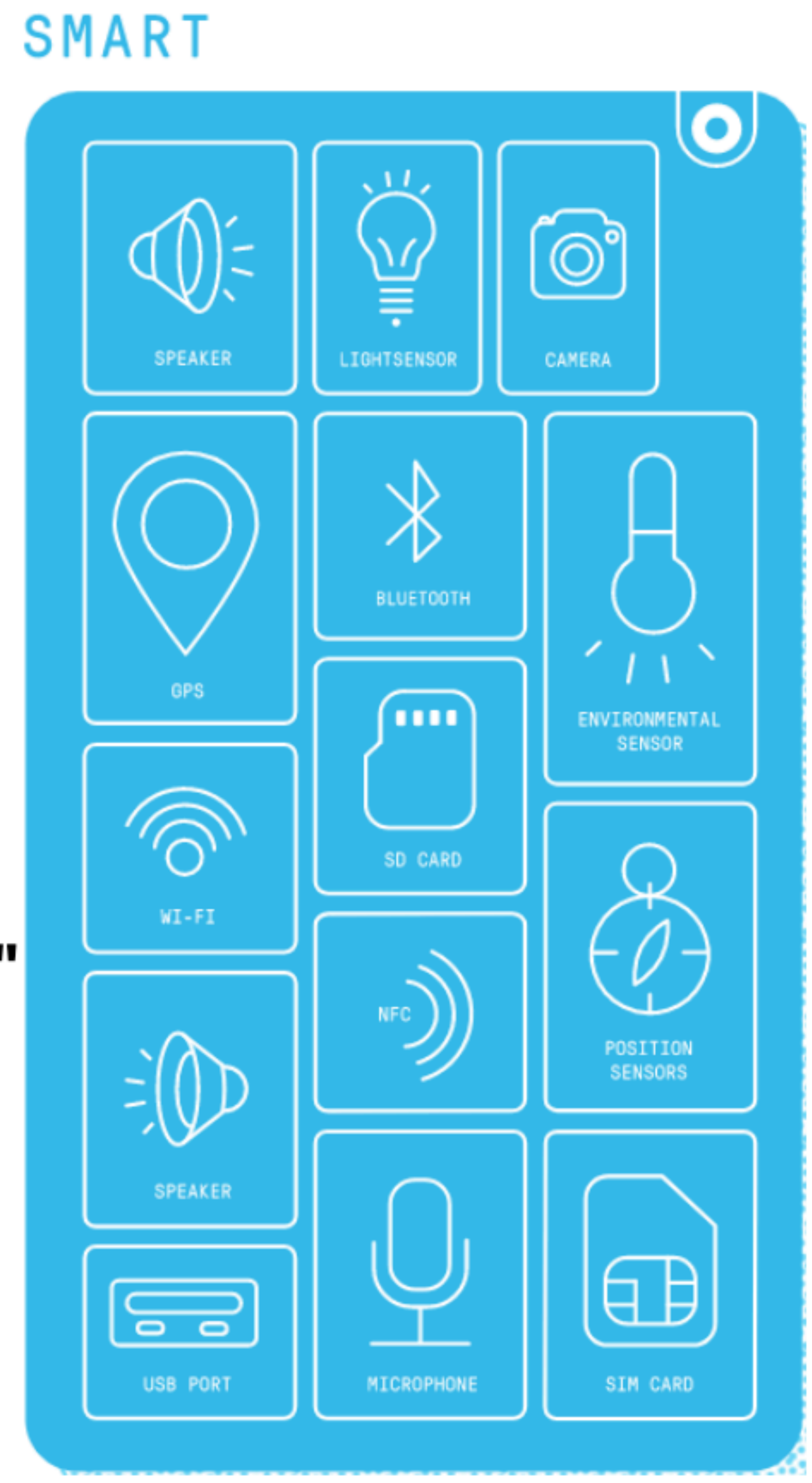
Similar to a flash drive

NFC- "Near Field Communication"

Can speak to devices within 4cm. e.g. used for payments.

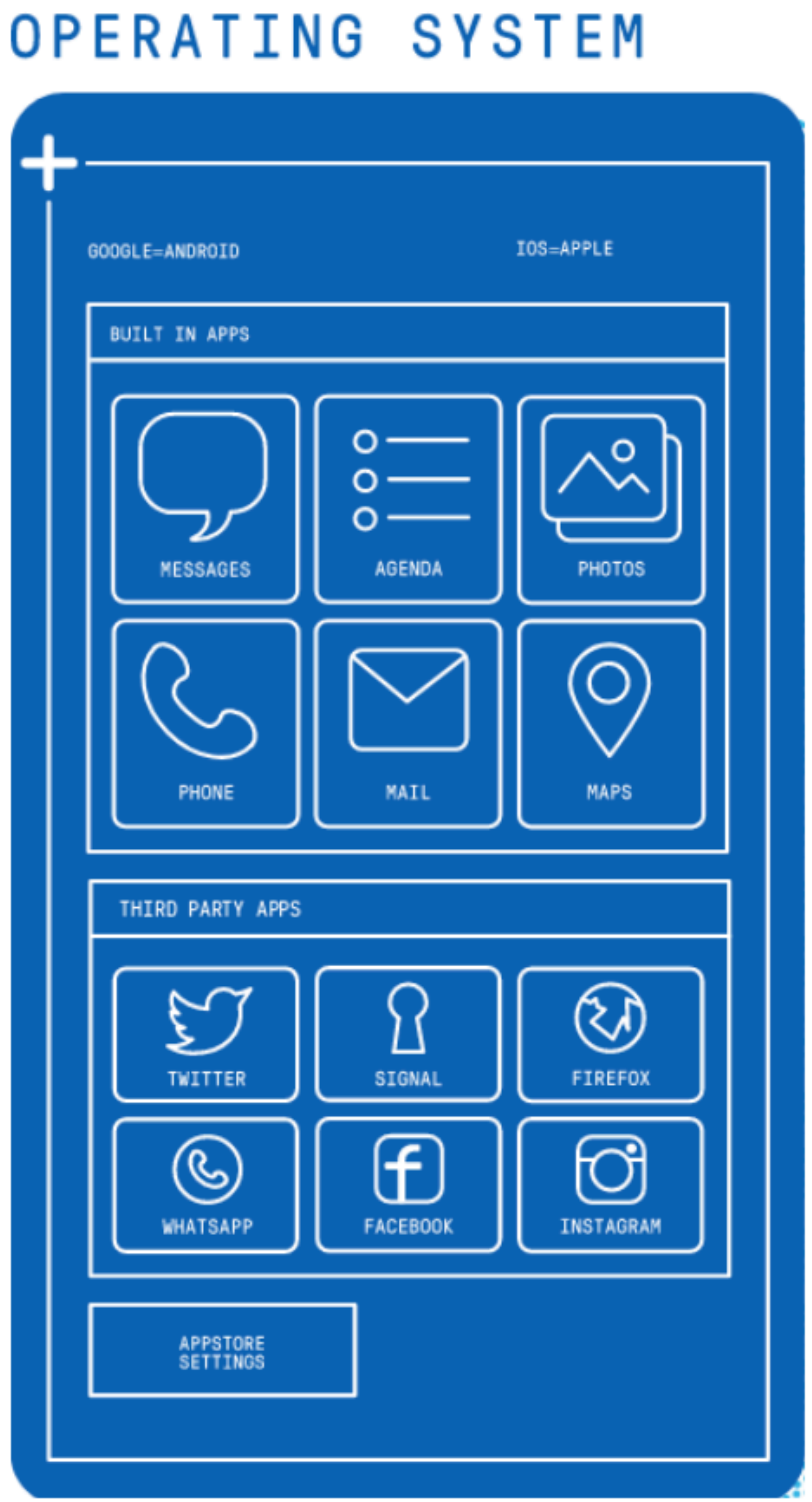
SIM card - "Subscriber Identity Module"

Unique card idenity, user identity when activated, contacts



Software

- Before this, any code was provided by the manufacturer(s), e.g. Samsung
- What are the differences between Android and iOS?
- What apps do you use?
    - Any apps you can't remove?
    - How many apps are ***proprietary*** v. ***"open"***?
    - Where do you get your apps?



Your info

- What information are you making available to your phone?
- What info is available to 3rd party programs?
- What info can be picked when your phone communicates with other devices?
- How is location tracked?

RISK ASSESSMENT

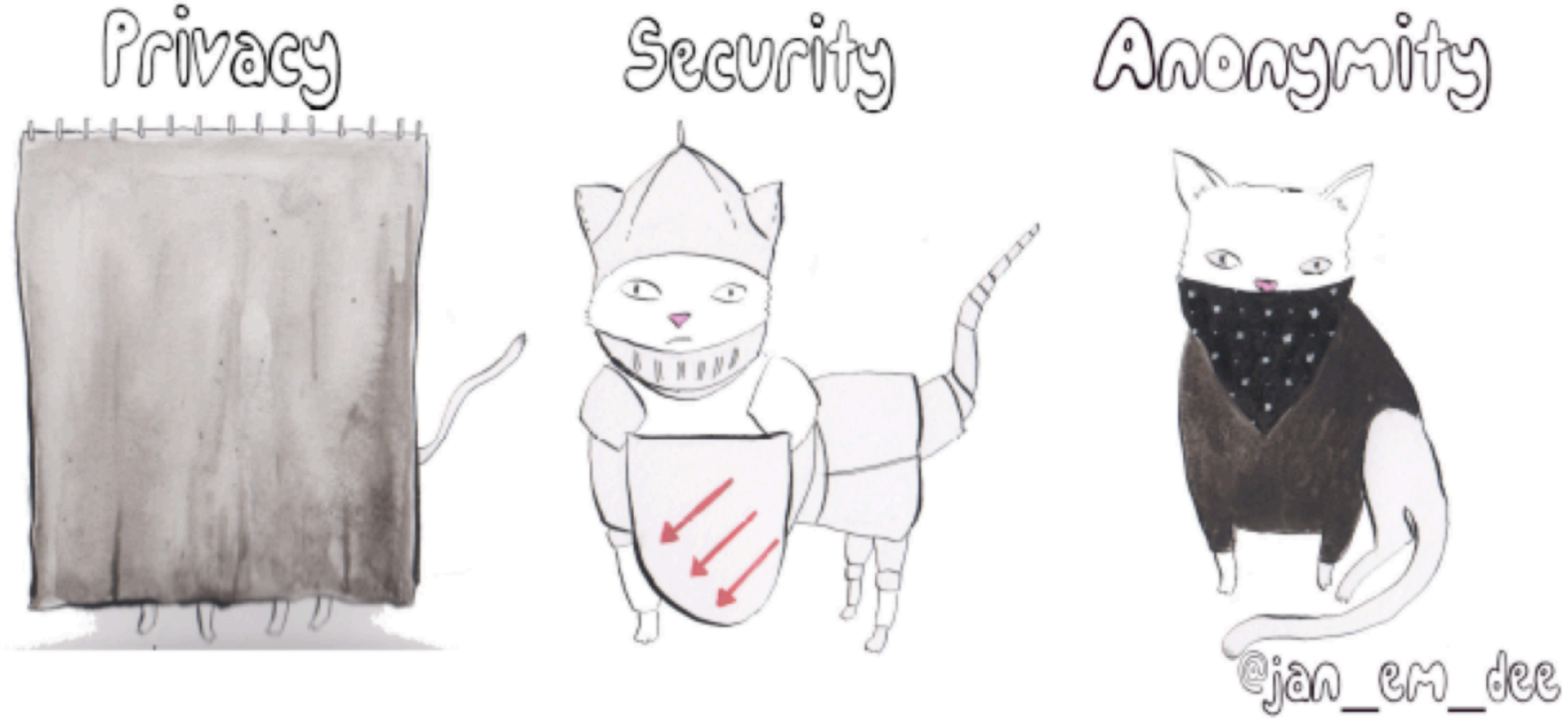
“What are you protecting?”

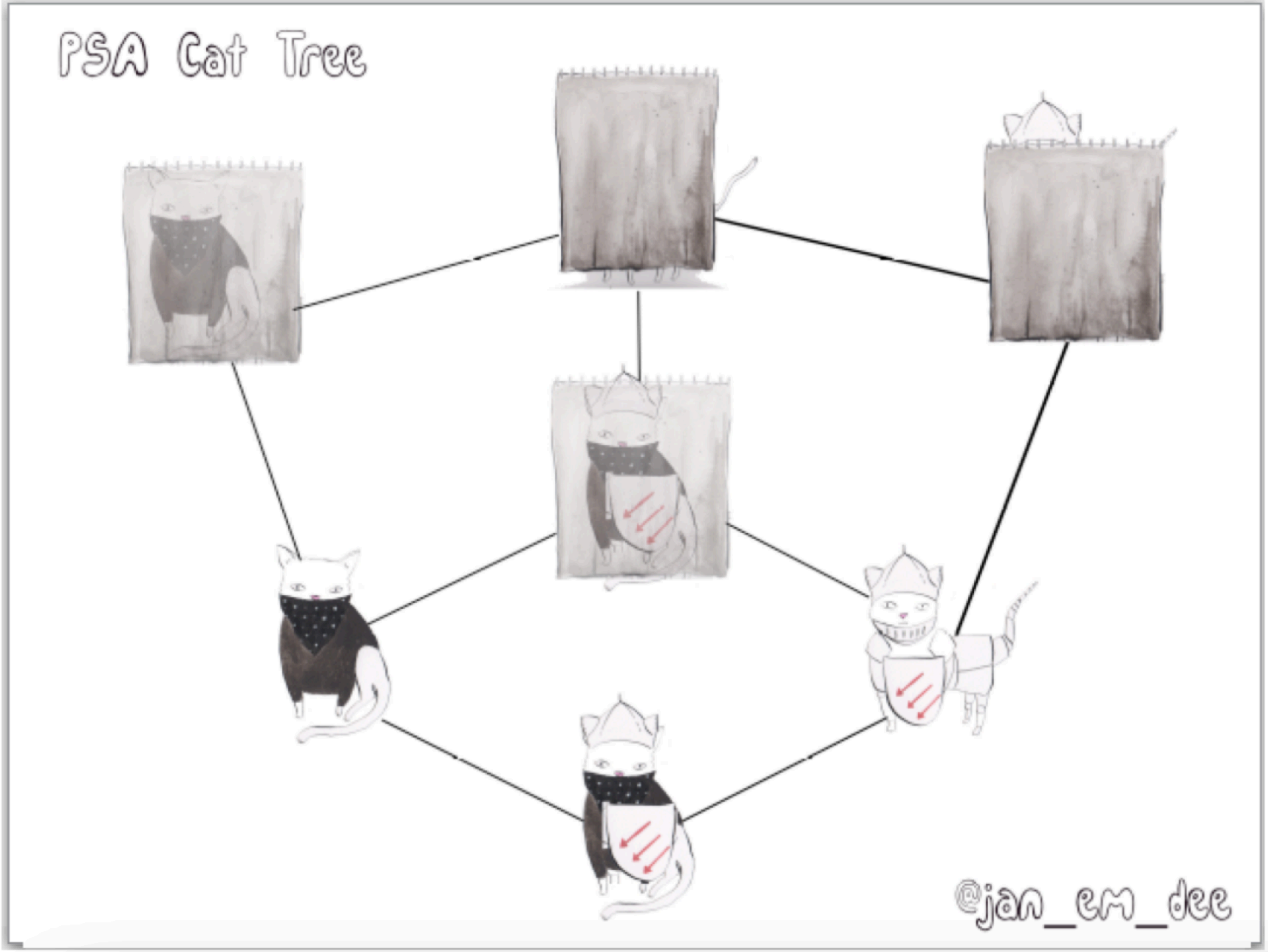
”Who are you protecting it from?”

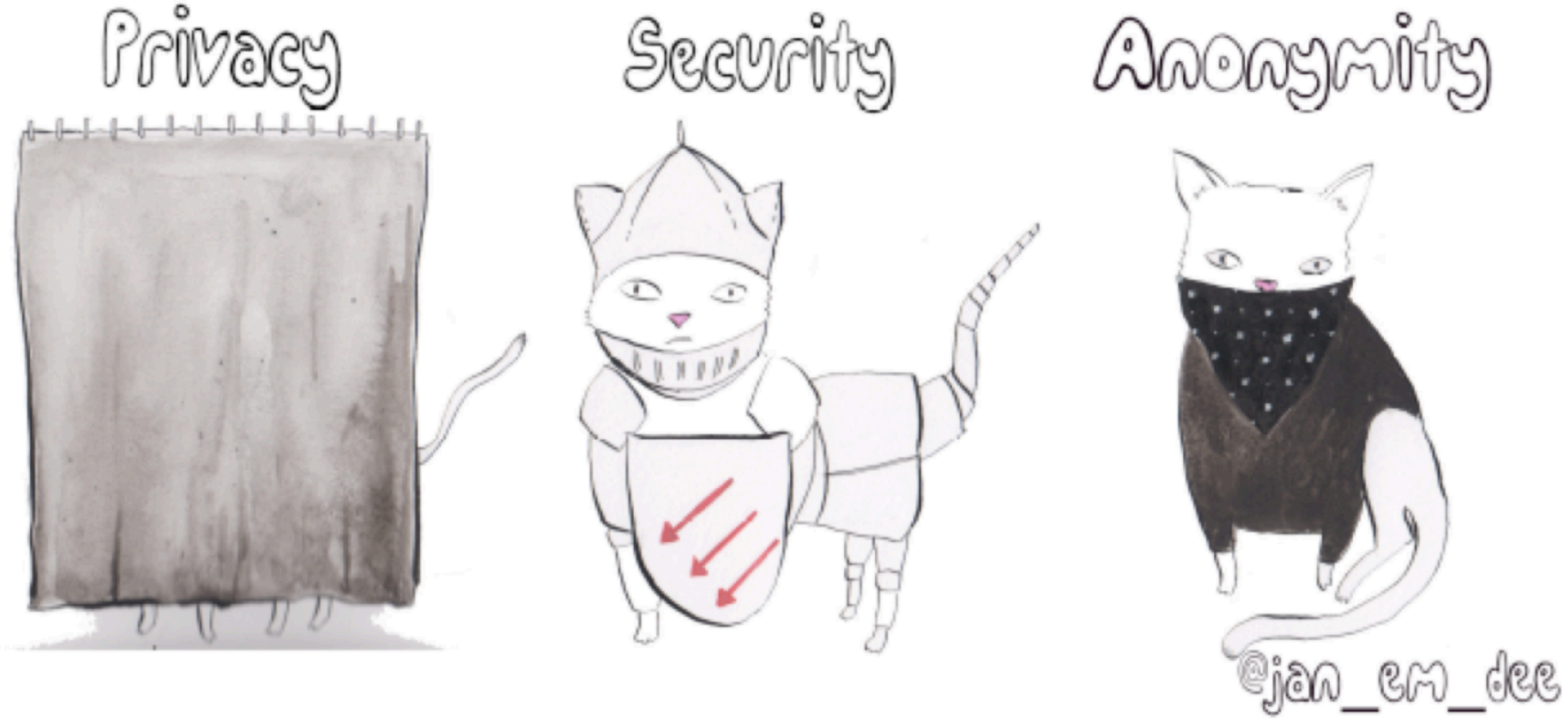
“What resources do they have to take it from you?”

“What are you willing to do to protect it?”

“What vulnerabilities do you need to fill to better protect it?”


Privacy
Security
Anonymity
@jan_em_dee


PSA Cat Tree
@jan_em_dee


Privacy
Security
Anonymity
@jan_em_dee


Privacy
Security
Anonymity
@jan_em_dee

Spying on Mobile Communications

Mobile phone networks were not originally designed to use technical means to protect subscribers' calls against eavesdropping. That meant that anybody with the right kind of radio receiver could listen in on the calls.

The situation is somewhat better today with encryption technologies have been added to mobile communications standards to try to prevent eavesdropping. But many of these technologies have been poorly designed (sometimes deliberately, due to government pressure not to use strong encryption). They have been unevenly deployed, so they might be available on one carrier but not another, or in one country but not another, and have sometimes been implemented incorrectly. For example, in some countries carriers do not enable encryption at all, or they use obsolete technical standards. This means it is often still possible for someone with the right kind of radio receiver to intercept calls and text messages as they're transmitted over the air.

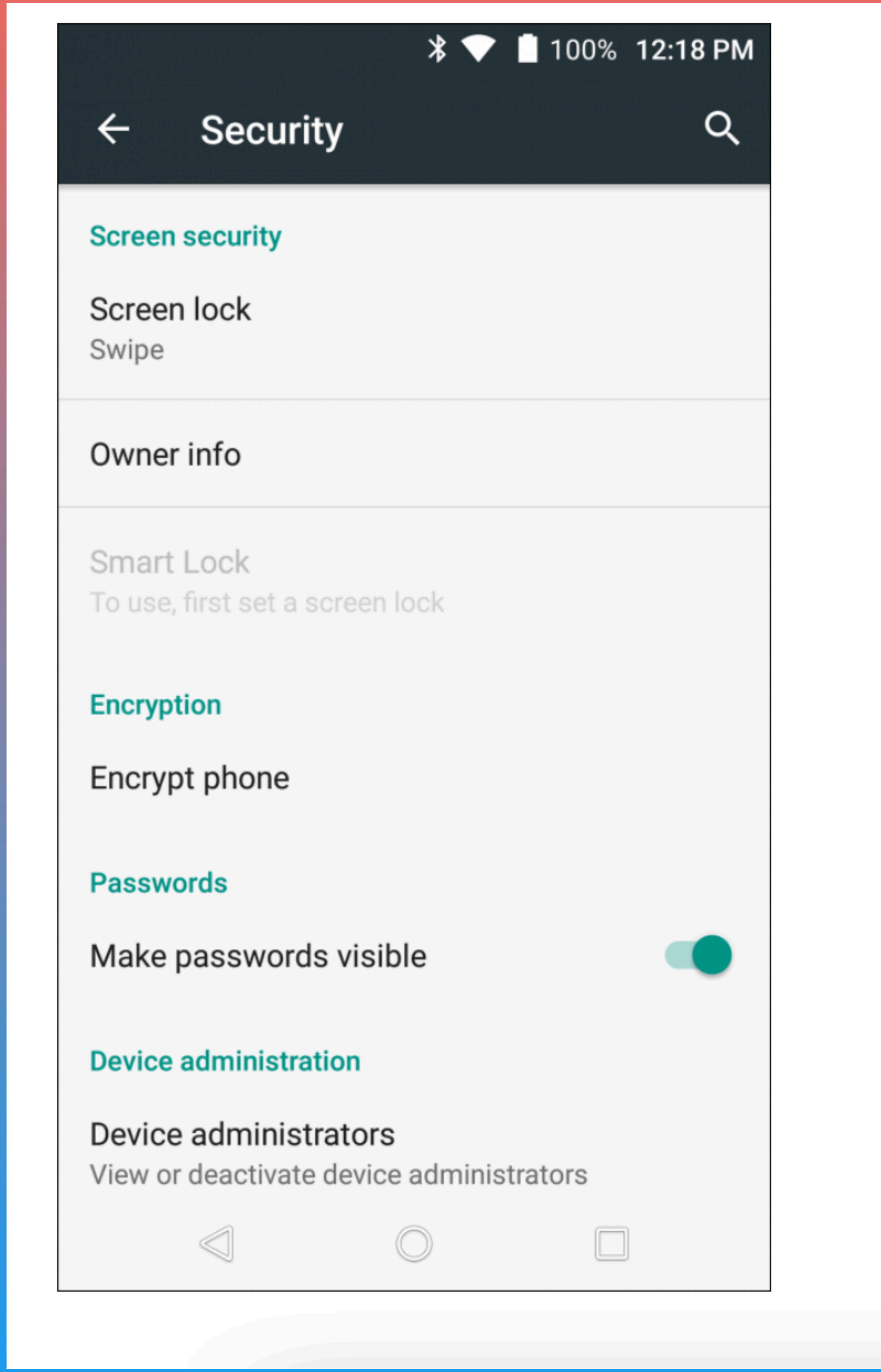
The safest practice is to assume that traditional calls and SMS text messages have not been secured against eavesdropping or recording. Even though the technical details vary significantly from place to place and system to system, the technical protections are often weak and can be bypassed in many situations.

It’s not just about **data**
It’s about ***habits***

Behavioral data collected from mobile apps is used primarily by advertising companies and data brokers, usually to do behavioral targeting for commercial or political ads. But governments have been known to piggyback on the surveillance done by private companies.

SECURITY SETTINGS

- Get to know your settings!
  - UPDATE YOUR PHONE!
  - Settings -> Security
    - Screen Lock
    - Phone Encryption
    - Sim Lock Options
    - Other



PASSWORDS!

- **Screen Lock**
  - Numeric/AlphaNumeric (6-10 characters)
  - Pattern
  - FaceID/Fingerprint
- **Password Managers**
  - BitWarden
- **2FA Apps**
  - Authy
  - Google Authenticator
  - FreeOTP

PASSWORDS!

Home > Categories > Cell Phone Bling / Charm Accessories > horchow > ***Item#:* 9SIASSACSV2083**

BodyGuardz - Spyglass Edge Privacy Screen Protector Extreme Edge-to-Edge Impact and Scratch Protection for iPhone Xs Max

Be the first to review this product...

Ask Or Answer A Question

SHARE

In stock.

Ships from China. Most customers receive within **5-17 days**.

- Cell Phone Bling / Charm Accessories

ACCESS

Digital Access

- **Malware**
  - Texts/Email
    - Be aware of links from unknown numbers and emails (spam? phishing?)
  - Unverified Apps
  - Access
    - Phone Content
    - Camera/Mic/GPS

Physical Access

- Who has access to your physical phone?

SIM SWAPPING

aka “simjacking”

The process of

- obtaining personal information on a user
- convincing their mobile carrier that the hacker is the user
- switching their SIM over to the attacker’s phone
- gaining access to info and accounts

SIM SWAPPING

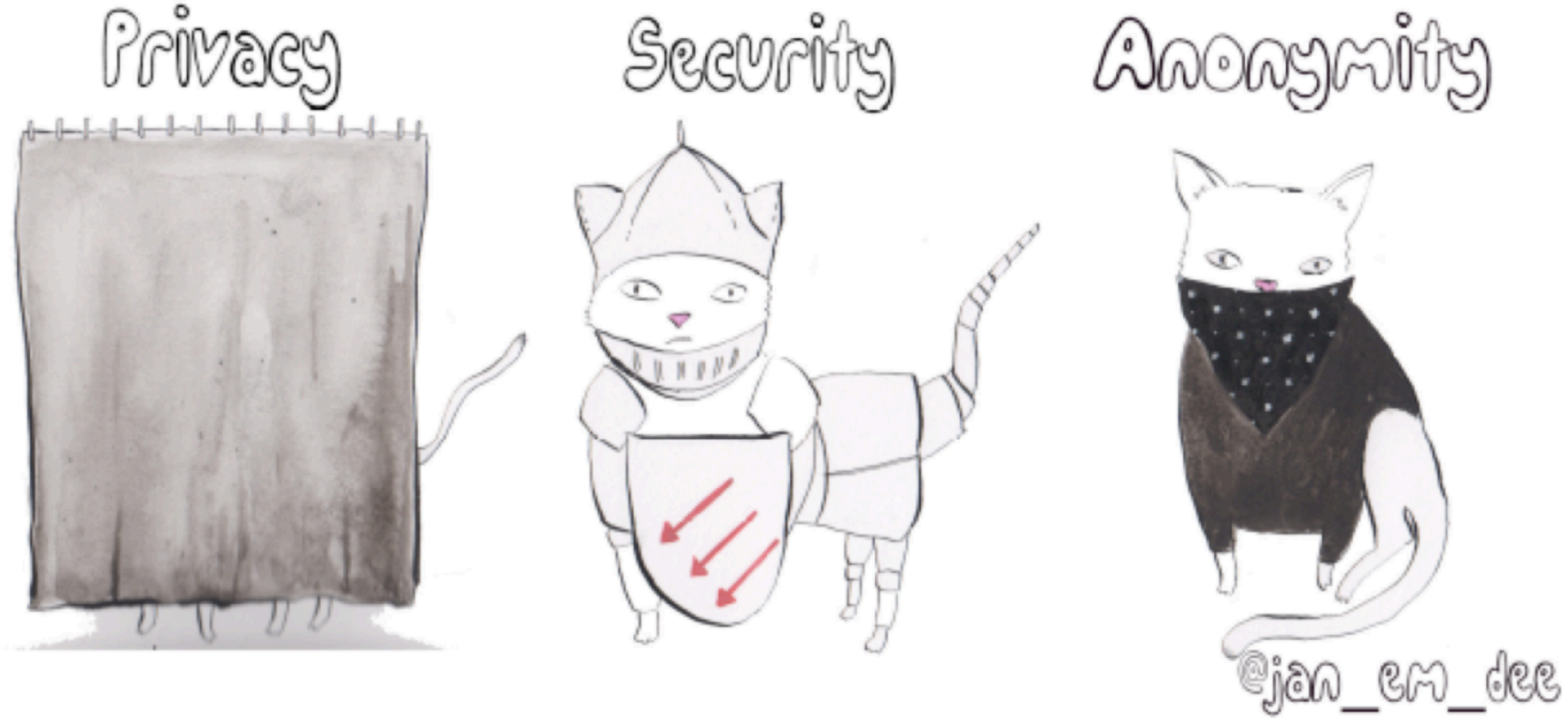
Information obtained through:

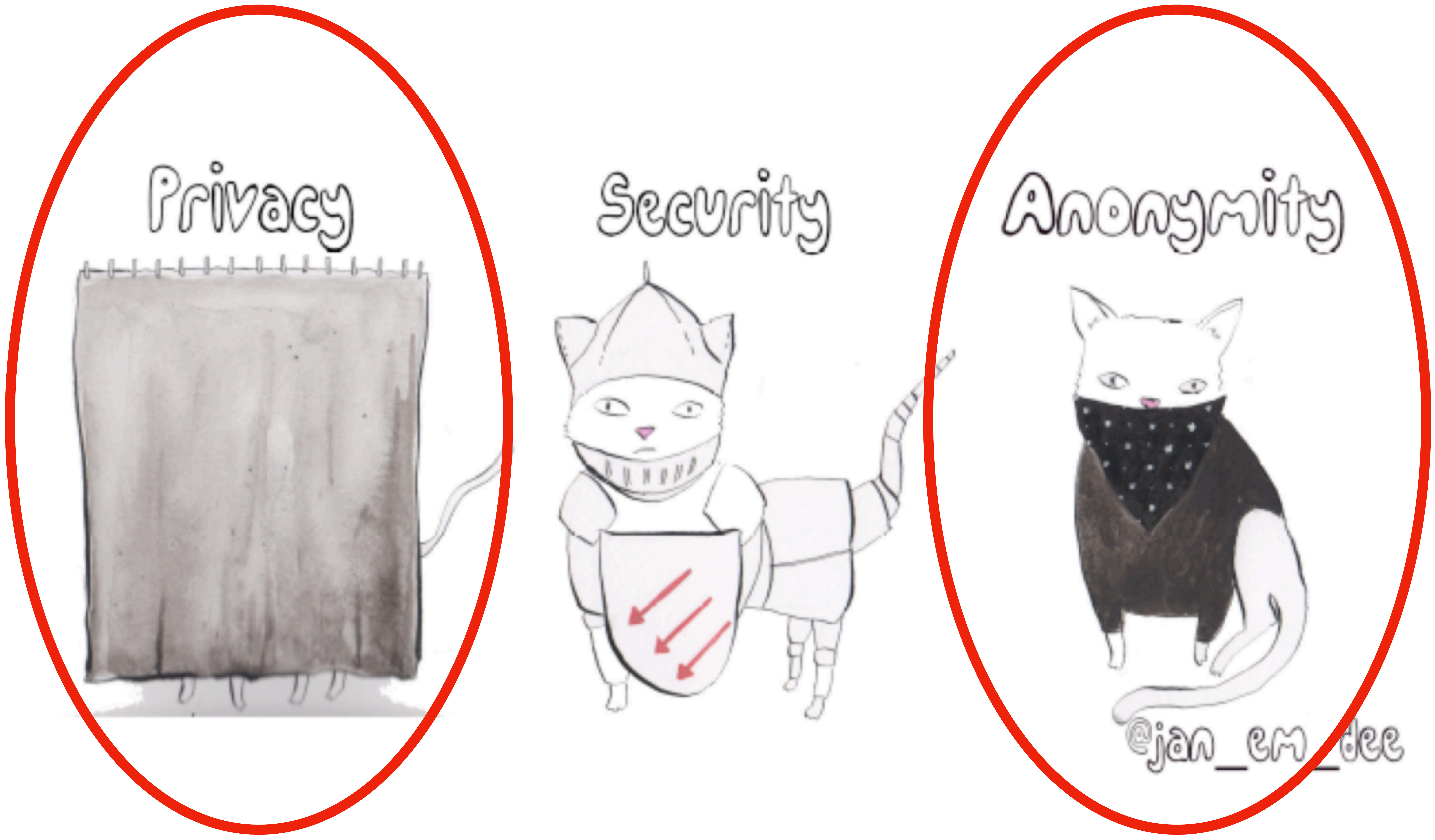
- **Online behavior**: phishing emails

Ways to Prevent

- **Account security**:, strong password and strong questions-and-answers (Q&A)
- **PIN codes**: set a separate passcode or PIN for your communications, consider doing it.
- **IDs**: Don’t build your security and identity authentication solely around your phone number.
- **Authentication apps**

- via Norton


Privacy
Security
Anonymity
@jan_em_dee


Privacy
Security
Anonymity
@jan_em_dee

SIMMER DOWN

Your phone constantly craves connection – with or without your participation. It's also really not picky about what it connects to: mobile networks, Wi-Fi networks, other devices (for example, through Bluetooth).

Your phone's approach to existence is to *broadcast continuously on every available open channel*: "I'm here! Over here! It's meeee!" – and to try to connect to any signals it can.

You may have even heard reports in the news about how **easy** it is for your personal data to get into just about anyone's hands.

But did you know **there are a few steps you can take** to reduce the amount of data you put out there?

Mobile Phones: Location Tracking

Location Tracking

The deepest privacy threat from mobile phones—yet one that is often completely invisible—is the way that they announce your whereabouts all day (and all night) long through the signals they broadcast. There are at least four ways that an individual phone's location can be tracked by others.

- Mobile Signal Tracking from Towers
- Mobile Signal Tracking from Cell Site Simulators
- Wi-Fi and Bluetooth Tracking
- Location Information Leaks from Apps and Web Browsing

DEVICE IDENTIFIERS

DON'T CALL ME BY YOUR NAME

At some point, you may have "named" your phone for *Wi-Fi, Bluetooth* or both – or maybe the name was automatically generated during setup.

This means that *"Alex Chung's Phone"* is what's visible to the Wi-Fi network owner and, if your Bluetooth is turned on, to everyone in the area who has their Bluetooth on as well.

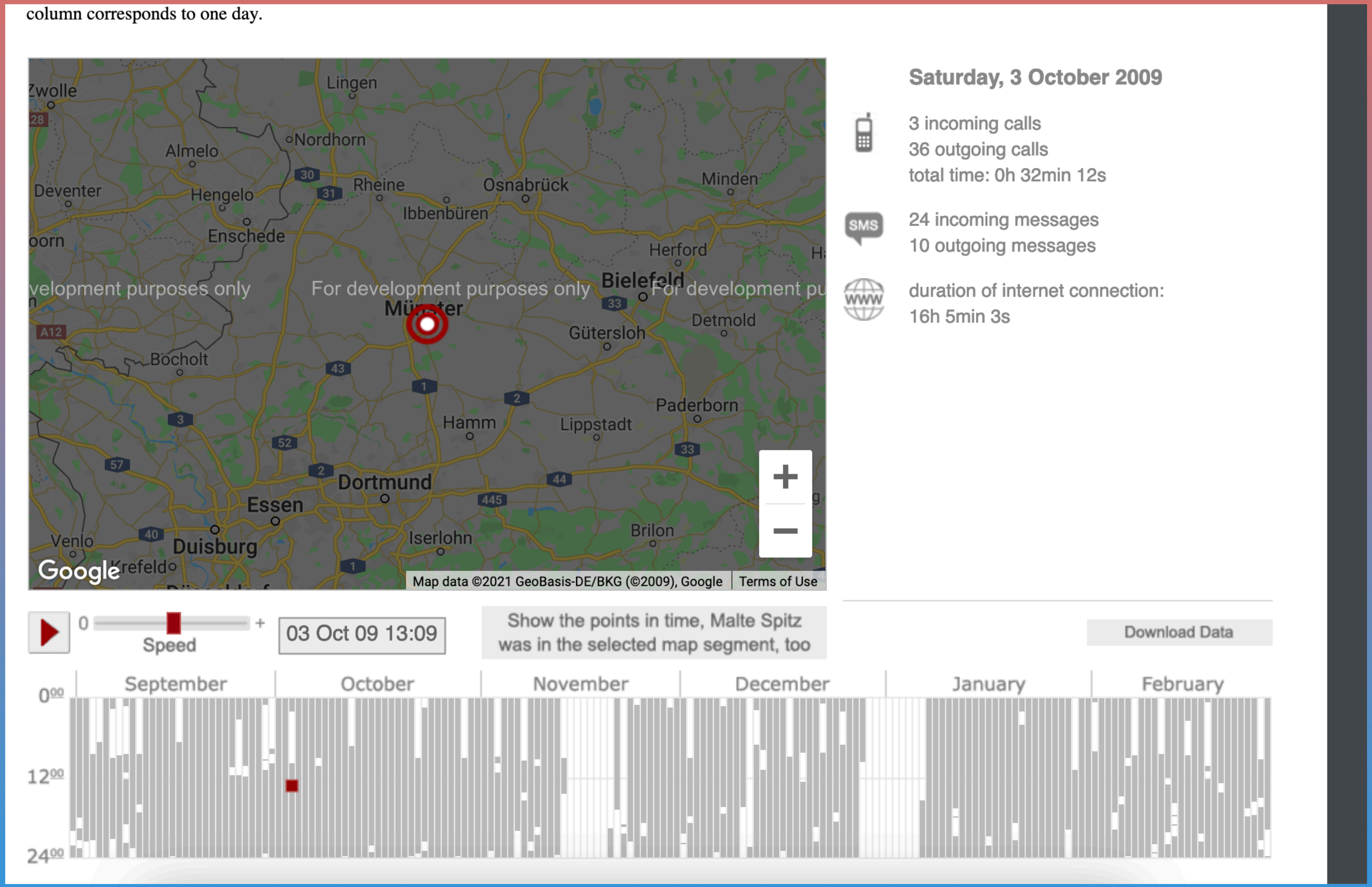
You wouldn't announce your name as you enter a café, restaurant or airport, so neither should your phone.

You can change the name of your phone to something less personally identifying, yet still uniquely you. Here's how:

APPS

Permissions/Settings

- Access to Phone
  - Contacts
  - Keyboard
  - Camera
  - Other Apps
- **Location Data**
  - Limiting/Deleting location information



APP CLEANSE!

(VIA DATA DETOX BY TTC)

Declutter Unwanted Apps

Limit Permissions

Replenish with Private Apps

Refresh and Renew!

PHONE BROWSING

To limit data gathered by phone

- Erase Browser Data
- Use Privacy-Friendly Browser (i.e. Firefox)
- Use browser vs. app
- Use computer vs. phone browser

BACKUPS

Spring Cleaning!

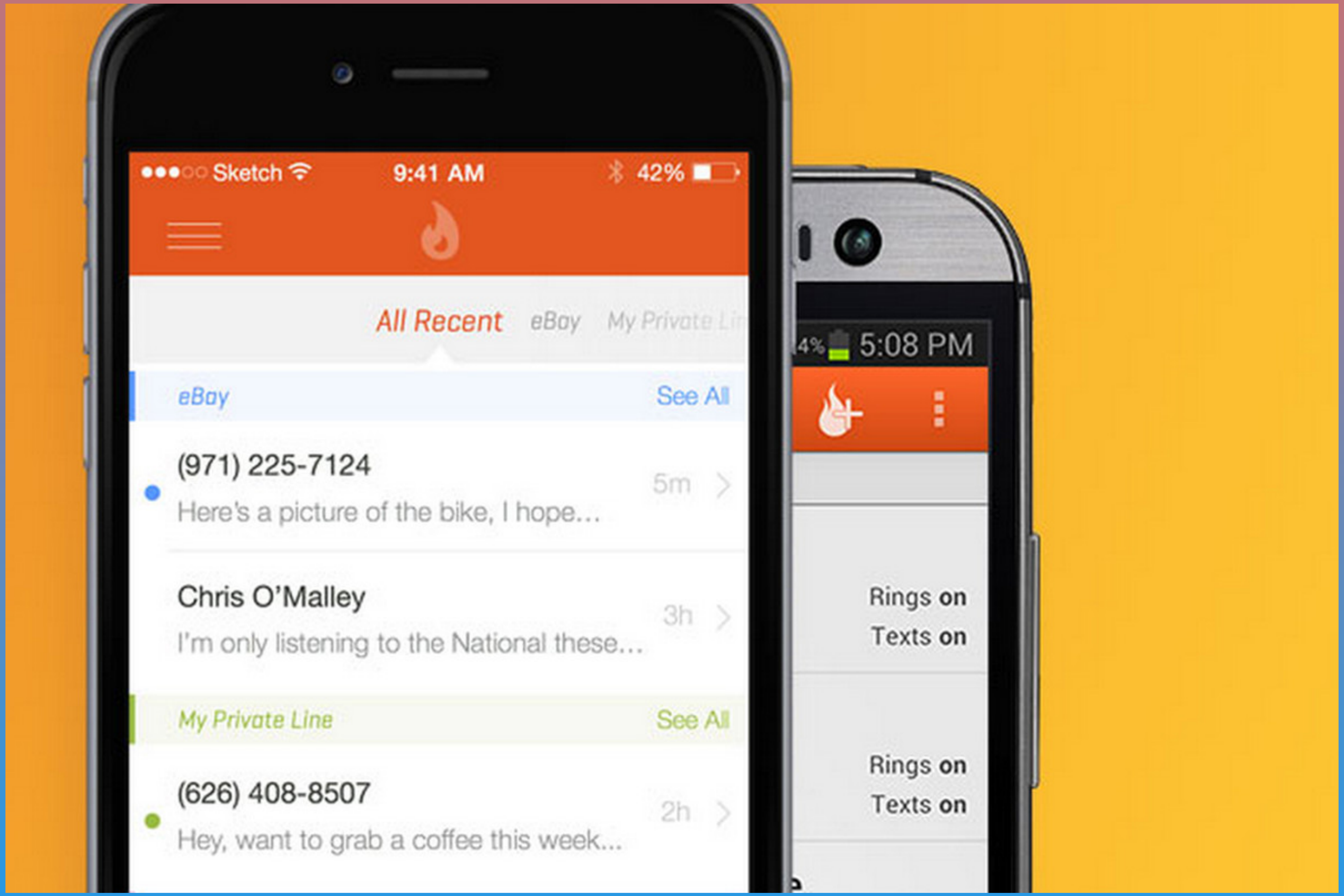
- Aware of what data is on your phone
  - Images/Videos
  - Files
  - Notes
  - Texts/Messages/Emails
- **Backup**
  - HardDrive Backup
  - Cloud Backup
    - Cryptomator

OTHER NUMBERS

Backup/Fake Phone Numbers

- Burner
- Google Voice

For use in situations where you don't want to give out your personal number



WHO ARE WE?

Cypurr Resources

Website- https://cypurr.nyc

Open Collective (Donation/Tshirt)- https://opencollective.com/cypurr-collective

Questions? Comments? Topic Ideas?

- Email- cypurr@protonmail.com
- Join our email list for updates!

Social Media- FB/Twtitter @cypurrnyc