THE TRIALS & TRIBULATIONS OF MAKING YOUR OWN PHONE

HOPE_16>

lamemakes

TLDR

- My journey trying to make a mobile phone in 2025
- ”Trials & Tribulations” and not ”How-To”
  - Incomplete project with hurdles (lots overcame already!)
- Highlighting software & hardware built
- Interesting privacy implications
  - Bringing users more agency
- Colored construction paper is fun

WHO AM I?

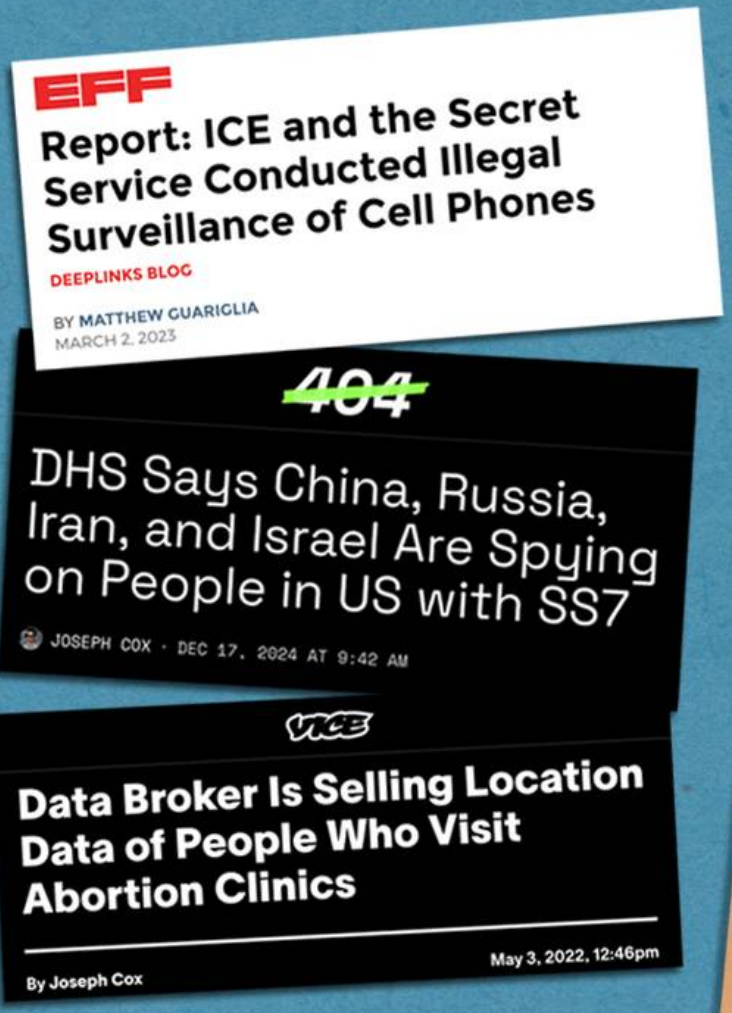
- Wes Appler
- Software dev @ Open Tech Fund
  - (views presented are all mine)
- Amateur hardware engineer
- FOSS advocate
- Hobby collector
  - Artist
  - Ham operator
  - Runner
  - Photographer
- New Brooklyn resident!

WHY BUILD A PHONE?

MISC. INTERESTS

- Learning…
  - to better utilize Rust
  - GSM networks' protocols, infrastructure & issues
  - designing RF hardware & PCBs
- Disconnecting
  - My smartphone draws too much of my attention
  - Felt too accessible at times

PRIVACY!



EFF

Report: ICE and the Secret Service Conducted Illegal Surveillance of Cell Phones

DEEPLINKS BLOG

BY MATTHEW GUARIGLIA
MARCH 2, 2023

~~404~~

DHS Says China, Russia, Iran, and Israel Are Spying on People in US with SS7

JOSEPH COX · DEC 17, 2024 AT 9:42 AM

VICE

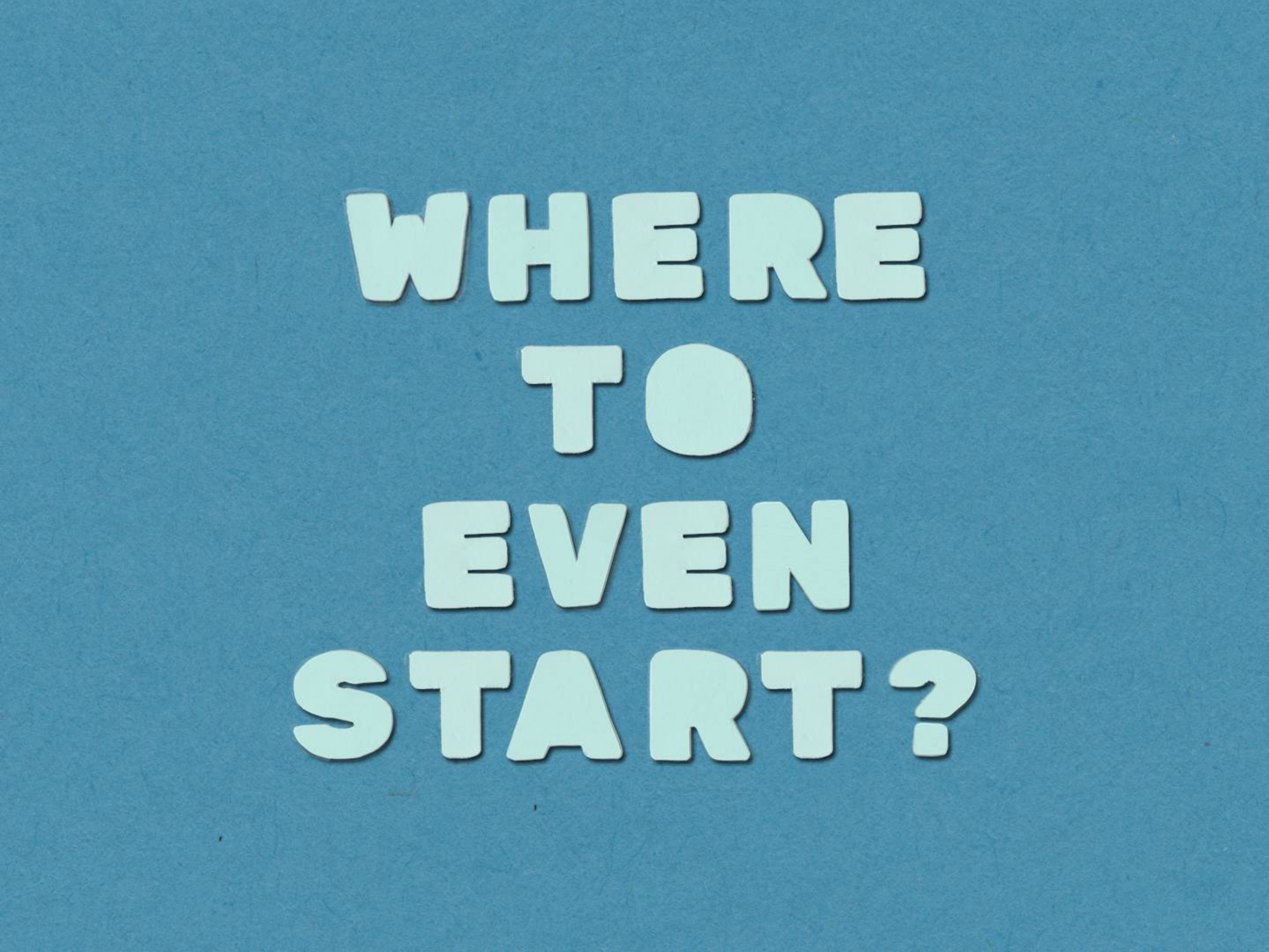
Data Broker Is Selling Location Data of People Who Visit Abortion Clinics

By Joseph Cox

May 3, 2022, 12:46pm

- Cell networks are insecure
  - SS7 is actively leaking data
  - Your location, calls & SMSs can be exposed
- Government surveillance
  - IMSI catchers pull UIDs, location data and more
  - Cops buy data from brokers
- Big tech data extraction
  - Assisted GPS/SUPL
  - Real time bidding

lamemakes

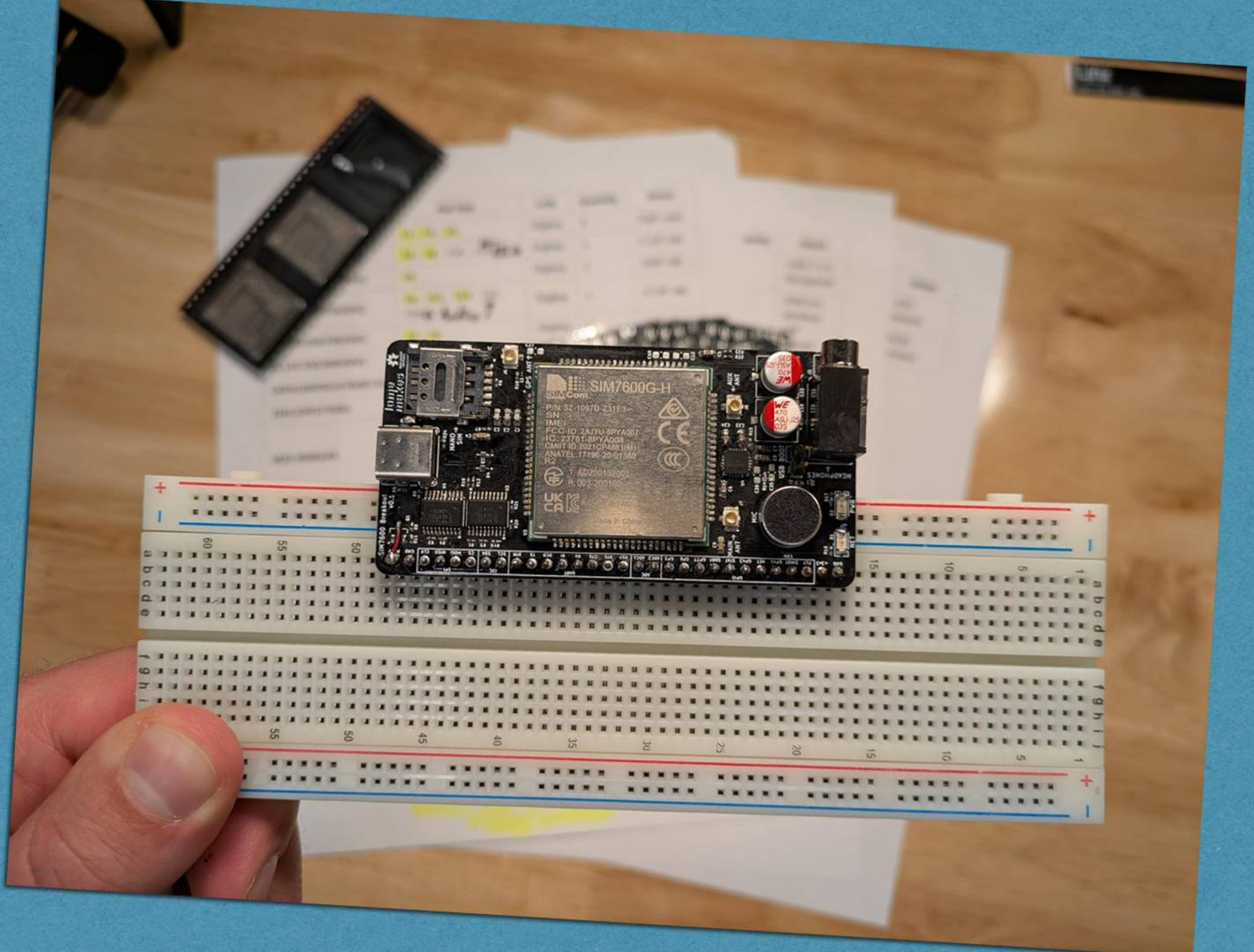

WHERE
TO
EVEN
START?

HARDWARE

- Finding and understanding modems
  - Datasheet paywall hell
  - SIM7600?
  - Unhelpful sales reps
  - When all else fails… fake an IOT startup!
  - Dragonfly Nano?
  - No carrier certification was ever needed
  - Baaaaack to the SIM7600

HARDWARE CONT.

- Building a development board
  - Exposing features of the SIM7600
  - V1 has...
    - Antennas broken out to external U.FL receptacles
    - USB-C 2.0 receptacle for interfacing
    - Nano SIM card slot
    - Headphone jack & on board mic
    - UART, I2C, & SPI voltage shifter
    - Labeled pins capatible with most breadboards
    - Indicator LEDs


SIM7600G-H
SIMCom

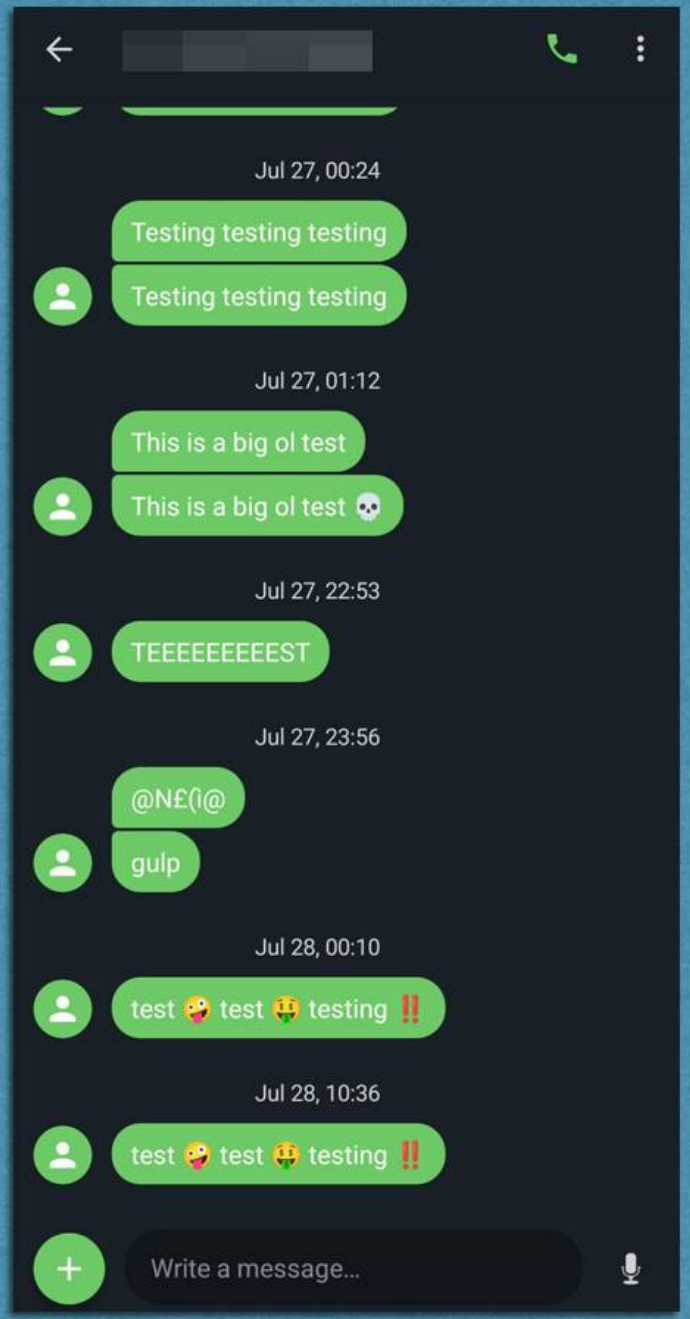

IT
DIDNT
EVEN
TURN
ON

SOFTWARE

- Communication with modem via UART
- What's a Hayes command set?
  - Developed in 1981 to interface with modems
  - Still used by modems today
  - Synchronous until it isn't
  - Somewhat difficult to develop for

SOFTWARE CONT.

- Needed an “abstraction layer”
- Started making a modem handler service in Rust
- Initial features include APIs for:
  - Sending & recieving SMSs - including emojis 🤪
  - Call handling (answering, ending, dialing)
  - IMEI getting & setting (more on this later)
  - Getting signal quality
  - Handling modem provided errors
- Uses tokio to handle Unsolicited Result Codes (URC)
- Had plans to expose APIs system wide via dbus


Jul 27, 00:24
Testing testing testing
Testing testing testing
Jul 27, 01:12
This is a big ol test
This is a big ol test 💀
Jul 27, 22:53
TEEEEEEEEEST
Jul 27, 23:56
@N£(i@
gulp
Jul 28, 00:10
test 😜 test 🤑 testing ‼️
Jul 28, 10:36
test 😜 test 🤑 testing ‼️
Write a message...

MODEM MANAGER..?

What is ModemManager?

ModemManager is a DBus-activated daemon which controls mobile broadband (2G/3G/4G) devices and connections. Whether built-in devices, USB dongles, bluetooth-paired telephones, or professional RS232/USB devices with external power supplies, ModemManager is able to prepare and configure the modems and setup connections with them.

NEXT STEPS

STANDALONE DEVICE

- Two types:
  - A price effective standalone device with embedded linux processor & modem onboard
  - Support for custom builds & swapping modems
- Wrapping all software services into an easily deployed package

ENCRYPTION

- Building a Signal client via Whisperfish's Presage
  - Would be the phone's default for comms
- Encrypting SMS in transit?
  - Encrypting the content of the message being sent
  - Could only be received by other phones/clients
  - Metadata is still exposed
- Encrypting data at rest by default (call history, SMSs, etc)

IMEI SPOOFING

I nternational

M obile

E quipment

I dentity

- A 15 digit IMEI is...
  - intended to be a unique device identifier
  - carrying info on a device's make/model
  - how a carrier determines device "compatibility"
  - carrier agnostic
  - used to track a device's activity
- spoofable!

IMEI SPOOFING CONT.

I nternational

M obile

E quipment

I dentity

- Some eSIM chips allow for 7+ different operator profiles
- Modems like the SIM7600 allow for setting of IMEI
- Changing IMEIs based on the operator profile makes a phone harder to surveil from a carrier's perspective
- ...and allows for more network compatibility!

STINGRAY SPOTTING

- Detecting Stringrays
  - Analyizing traffic from modem & base station
  - Notifying user of strange activity (ie. 2G downgrade requests)
- Custom built or (ideally) making the platform compatable with EFF's Rayhunter

GET INVOLVED

No formal channels for organizing yet but...

email me!

wes@lamemakes.com

website w/ RSS

lamemakes.com