# Unshackling 2: Securing Communications

April 10, 2026

# Outline

# Overview

- The state of our one to one and group communications is pretty bad. They're not private and easily used against us by governments and corporations.
- Not to worry! We have, uh, *less bad* options available!
- No wait really, some are even quite good.

# Concepts

- Plain-text – Just bytes flyin' around for anyone to see.
- TLS encrypted – Data is encrypted in transit between nodes, but not necessarily on the devices or server.
- End-to-end encryption (E2EE) – *only* the sender and recipient can read the data. Nobody in between, even the provider server, can read the data. Ideally also encrypted on disk for users.
  - Implemented correctly, this really works. You can't realistically simply "hack" proper encryption (though there may be other methods of obtaining the data), even if you're a mad genius or the feds.
- Zero-access – sounds cooler but is a little worse. "We could read your stuff, but we're choosing not to." Provider can't physically hand over your data.

# SMS

SMS is bad. It's really bad. This is the original protocol for texting between phones, still sometimes used between Android and iPhone or when data/wifi not available.

- Unencrypted. Plain-text.
  - You might as well shout into the street. No wait, that would be *more* secure.
- Pretty easy to spoof and spy on.
  - I wouldn't personally know how but like, trust me it's true.
- Even ignoring the above it's generally pretty `garbage.jpeg`.
  - Message size limits, shitty compression on multimedia (MMS), no read receipts if you're into that (I'm not really), etc.

# iMessage

iMessage is Apple's own end-to-end encrypted (E2EE) protocol.

- iPhone only. Let's move on.
- (And a proprietary implementation purely dictated by a private company)

# RCS

*Technically* an open protocol to rival iMessage! Can incorporate E2EE! Works between Android and iPhone!

. . . oh wait:

- E2EE is *not* part of the standard, but implemented by Google between Android phones.
  - Not E2EE between iPhone and Android.
  - It *is* still TLS encrypted, which is better than SMS
- Most people will rely on Google and Apple's proprietary implementations.

# Whatsapp

- . . . is owned by Meta (Facebook).
- Yes, okay, it's end-to-end encrypted.
- But it's proprietary and owned by *Facebook*.
- "I'll take top 5 companies that couldn't possibly care any less about you for 200, Alex!"

# Discord

- Technically TLS encrypted in transit between you $\leftrightarrow$ server $\leftrightarrow$ recipient, but is not encrypted on the server.
- Will start requiring face scans with allegedly limited but extremely dubious scope.
- Low-key trying to monopolize and monetize group chats? Despite being initially targeted towards gamers.
  - Hey also remember teamspeak? idk that was a thing for a hot second
  - RIP Skype I guess

# Gmail

- TL;DR: Same issues as Discord, but email; no encryption on server.
- Google can and does read all your messages on their server... yaaay (sarcasm)
  - e.g. automatically generating calendar invites from flight confirmation email.
  - Most recently for training AI, but who knows for what else.
- Same goes for Outlook, Hotmail (wait do ppl still...), hey remember Yahoo mail?

# Why do you care, Diego? Why should I care?

*Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.*

- Edward Snowden*

*Not a wholesale endorsement of this figure.

# The problem

- The government can and does collect your information, legally or illegally, via proprietary software and agreements with (or demands to) private companies.
  - This isn't a conspiracy or paranoia; the PRISM program is only one example of an ongoing mass surveillance program whereby the NSA can access baaasically all your unencrypted internet data.
  - All the for-profit companies mentioned in this presentation are implicated, among others.
  - Queer, Black, and Latino people have practically always been systematically targeted and things are not looking great these days.
- When companies implement E2EE in proprietary software, we simply have to "take their word" for it. We don't know what corners they cut or backdoors they implement, especially when they *literally* make a profit from your data.

# Why open-source software is a better solution

- Popular open-source software is examined and vetted by thousands of people, including many experts. Less popular open-source software at least has the ability to be scrutinized in the same way.
- Since uncapped profit or growing market share are not the goal, lots of open-source software is written with the public good and specifically privacy in mind.
  - It's also often written by people who either genuinely enjoy doing it or have very strong convictions around it.
- It's more resistant to centralization, monopoly, and and puts the power in the hands of the people (e.g. you can fork, self-host, locally modify, whatever).

# Signal instead of SMS (or other DM software)

## The good

- State of the art, post-quantum encryption that sets the standard. In fact, Google RCS, iMessage, and Whatsapp *allegedly* all use the Signal Protocol.
- Has undergone regular academic and informal audits.
- Collects almost no metadata (e.g. info about contacts, groups, times)

## The imperfect (but don't let perfect be the enemy of good)

- Requires and stores your phone number in order to work.
- Signal is fairly centralized, relying on one main implementation and infrastructure and not really designed to be federated.

# Matrix instead of Discord(?)

## The good

- Encrypted DMs and optionally encrypted group chats.
- Can be organized into "spaces" and "rooms" like Discord.
- Federated protocol, which means it's designed to be self-hosted in multiple servers that can communicate with each other. This makes it have less of a central point of failure.

## The imperfect (but don't let perfect be the enemy of good)

- Growing pains; it's seen pretty slow adoption due to implementation bugs and difficulties to users.
- *Good lord* is it a pain to set up self-hosting. Maybe a skill issue?

*There are alternatives like Stoat (not encrypted, pretty young), Rocket Chat (sorta open, sorta not?), Mattermost (same)

# Protonmail instead of Gmail

## The good

- End-to-end encrypted email based in Switzerland.
- Open-source front ends and clients.
- Falls back to zero-access; encrypts all incoming mail on their server.

## The imperfect (but don't let perfect be the enemy of good)

- Backend is closed source :( but still third-party audited.
- Less space in free tier than Gmail, but fairly reasonably priced plan options.

## Alternatives

- Tuta offers a similar service, same basic idea. Still a technically closed-source backend.

# So... do the thing!


- Encourage your circle to use Signal instead of SMS, iMessage, RCS, or Whatsapp.
- Try Matrix instead of Discord (and join our matrix.org space!).
- Check out Proton or Tuta instead of Gmail.
- *Do not* just take my word for this. Do some web searches, read some Wikipedia articles, blog posts, etc. Find opinions from field experts.

# Encrypted, peer-to-peer communications

- Peer-to-peer (P2P) encrypted communications are sometimes considered even better than centralized (or federated) encrypted messaging.
- P2P implies that messages hop from device to device, ultimately only ending up at the destination and never any servers (centralized or federated).
- This means the infrastructure *is* the users.
- This is neat, but I don't know of messaging-specific P2P software with a solid enough reputation to recommend.

# Other forms of communication

- For social media, Mastodon and Bluesky are open-source and federated alternatives to twitter that can't just be, like, bought by Elongated Muskrat.
  - Not encrypted for obvious reasons, meant to be more of a pulbic microblogging platform.
- IRC (Internet Relay Chat, e.g. libera.chat) is an internet messaging protocol that's been around since the late 80's. It's not at all encrypted beyond TLS, but there are still active communities of programmers and open-source enthusiasts there.

# Where encryption falls short

*Encrypted messaging apps are a superb tool to protect yourself against mass surveillance. Targeted surveillance is another matter. A sufficiently determined (and resourced) adversary will [likely] succeed.*

- Someone online, idk

- Encryption really does work, but that doesn't make it all-powerful. More often than not there are other ways to get your information:
  - Unencrypted recipients (e.g. email from ProtonMail to Gmail)
  - Using a mobile keyboard like gboard that send some info back to company servers. *Allegedly* it does not send actual message contents.
  - Phishing and other forms of social engineering.
  - Blackmail or physical violence