Security/privacy workshop

For activists

Why does it matter?

Where are we at?

- Surveillance capitalism is now the most powerful form of capitalism
  - Google
  - Facebook
  - Microsoft
  - Twitter
  - Amazon
- You are tracked by these companies everywhere you go on the internet
- Steal data —> Model you —> Predict your behaviour —> Sell your attention **for whatever purpose pays**
- This works better **if they change your behaviour and how/what you think too**

Behaviour modification

- Who chooses the new behaviour? Very rich, climate denying, neoliberal capitalists
- This goes way beyond targeting ads to sell things:
  - Cambridge Analytica + Facebook: Vote Leave (Brexit)
  - Cambridge Analytica + Facebook: 2016 US election
  - Fossil fuel companies
- It specialises in spreading misinformation and polarising people, all for the profit of a few rich people (usually in Silicon Valley)
- Surveillance capitalism is destroying democracy

See it for yourself

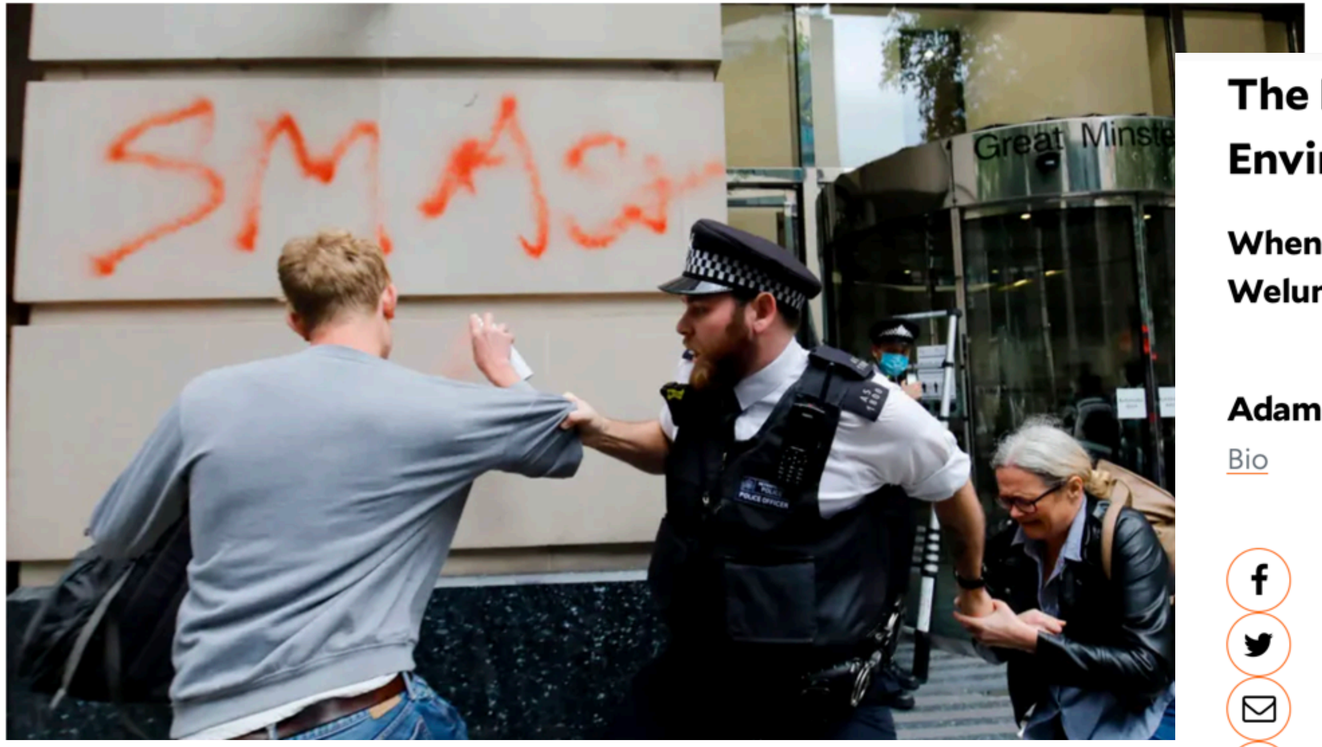
- The Social Dilemma (1.5 hours): https://www.netflix.com/title/81254224
- The Great Hack (1.5 hours): https://www.netflix.com/title/80117542
- The Age of Surveillance Capitalism: https://www.worldofbooks.com/en-gb/books/professor-shoshana-zuboff/age-of-surveillance-capitalism/9781781256855

This is bad

But you are also an activist, so it’s worse.

- It erodes democracy and the right to protest
- The information gathered will be used against you to sabotage protest efforts
- There are companies that specialise in monitoring activists and report back to governments and (oil) companies
  - https://www.standard.co.uk/news/politics/welund-city-hall-london-xr-b74225.html
  - https://www.dailykos.com/stories/2018/9/17/1796352/-The-Fossil-Fuel-Industry-is-spying-on-environmental-activists-and-organizations
- The information will also be used against you in court

City Hall faces questions over contract with spy firm gathering intelligence on protests



The Private Intelligence Firm Keeping Tabs on Environmentalists

When big oil companies want to monitor activists, they turn to Welund.

Adam Federman

Bio

Scare stories!

It’s clear: we need security and privacy

It’s not too hard to get it

- We need to secure:
  - Devices
  - Communication
  - Storage
  - Using the internet (browsing, searching, watching)
- Every person who is secure and private:
  - Keeps themself safe
  - Keeps every single activist they communicate with safe
- It takes one person to endanger an entire network of people

Communication

Signal
'Data Linked To You'

iMessage
'Data Linked To You'

Contact Info
- Email Address
- Phone Number

Search History

Identifiers
- Device ID

WhatsApp
'Data Linked To You'

Analytics

- Purchases
  - Purchase History
- Location
  - Coarse Location
- Contact Info
  - Phone Number
- User Content
  - Other User Content
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
  - Advertising Data
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data

App Functionality

- Purchases
  - Purchase History
- Financial Info
  - Payment Info
- Location
  - Coarse Location
- Contact Info
  - Email Address
  - Phone Number
- Contacts
  - Contacts
- User Content
  - Customer Support
  - Other User Content
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data

Facebook Messenger
'Data Linked To You'

Third-Party Advertising

- Purchases
  - Purchase History
- Financial Info
  - Other Financial Info
- Location
  - Precise Location
  - Coarse Location
- Contact Info
  - Physical Address
  - Email Address
  - Name
  - Phone Number
  - Other User Contact Info
- Contacts
  - Contacts
- User Content
  - Photos or Videos
  - Gameplay Content
  - Other User Content
- Search History
  - Search History
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
  - Advertising Data
  - Other Usage Data
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data
- Other Data
  - Other Data Types

Analytics

- Health & Fitness
  - Health
  - Fitness
- Purchases
  - Purchase History
- Financial Info
  - Payment Info
  - Other Financial Info
- Location
  - Precise Location
  - Coarse Location
- Contact Info
  - Physical Address
  - Email Address
  - Name
  - Phone Number
  - Other User Contact Info
- Contacts
  - Contacts
- User Content
  - Photos or Videos
  - Audio Data
  - Gameplay Content
  - Customer Support
  - Other User Content
- Search History
  - Search History
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
  - Advertising Data
  - Other Usage Data
- Sensitive Info
  - Sensitive Info
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data
- Other Data
  - Other Data Types

Product Personalisation

- Purchases
  - Purchase History
- Financial Info
  - Other Financial Info
- Location
  - Precise Location
  - Coarse Location
- Contact Info
  - Physical Address
  - Email Address
  - Name
  - Phone Number
  - Other User Contact Info
- Contacts
  - Contacts
- User Content
  - Photos or Videos
  - Gameplay Content
  - Other User Content
- Search History
  - Search History
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
  - Advertising Data
  - Other Usage Data
- Sensitive Info
  - Sensitive Info
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data
- Other Data
  - Other Data Types

App Functionality

- Health & Fitness
  - Health
  - Fitness
- Purchases
  - Purchase History
- Financial Info
  - Payment Info
  - Credit Info
  - Other Financial Info
- Location
  - Precise Location
  - Coarse Location
- Contact Info
  - Physical Address
  - Email Address
  - Name
  - Phone Number
  - Other User Contact Info
- Contacts
  - Contacts
- User Content
  - Emails or Text Messages
  - Photos or Videos
  - Audio Data
  - Gameplay Content
  - Customer Support
  - Other User Content
- Search History
  - Search History
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
  - Advertising Data
  - Other Usage Data
- Sensitive Info
  - Sensitive Info
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data
- Other Data
  - Other Data Types

Other Purposes

- Purchases
  - Purchase History
- Financial Info
  - Other Financial Info
- Location
  - Precise Location
  - Coarse Location
- Contact Info
  - Physical Address
  - Email Address
  - Name
  - Phone Number
  - Other User Contact Info
- Contacts
  - Contacts
- User Content
  - Photos or Videos
  - Gameplay Content
  - Customer Support
  - Other User Content
- Search History
  - Search History
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
  - Advertising Data
  - Other Usage Data
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data
- Other Data
  - Other Data Types

Communication - main points

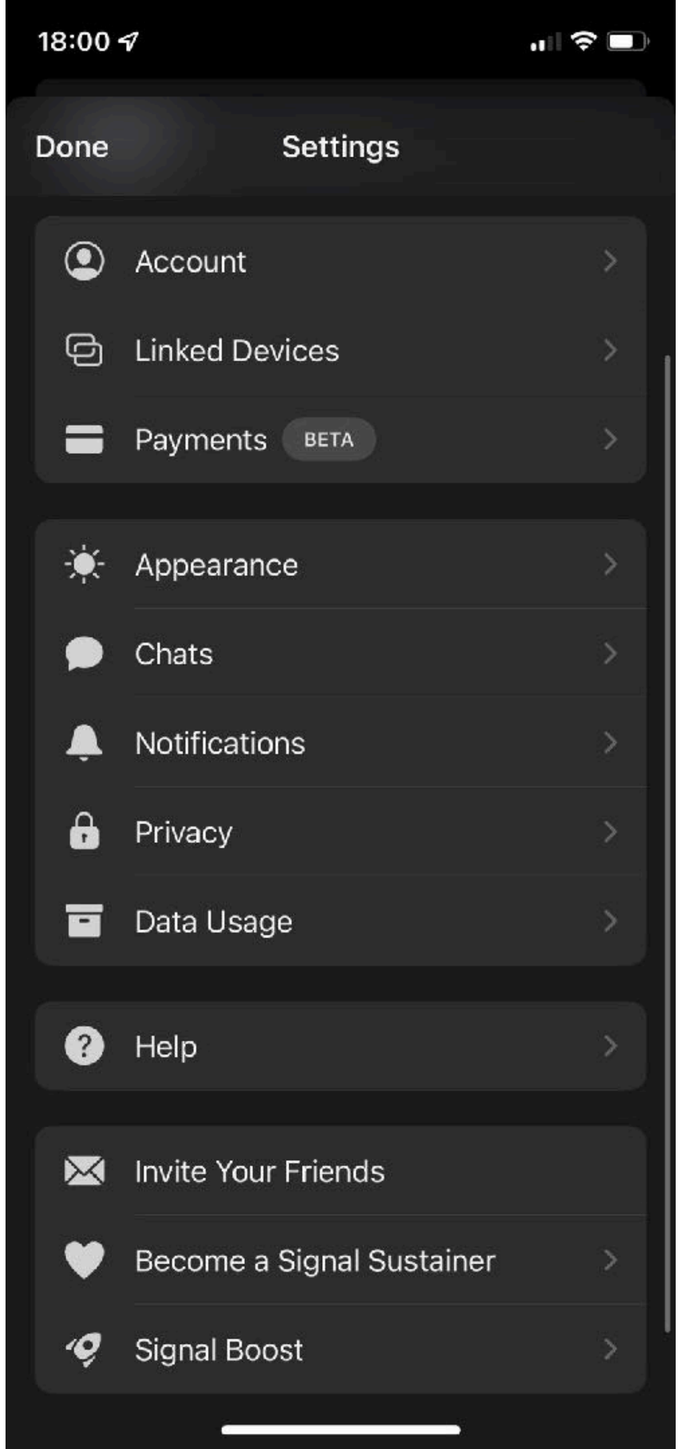
- For calling and messaging people/groups:
  - Use Signal by default
  - **Definitely** avoid Facebook Messenger and SMS texts
  - Avoid WhatsApp if possible
  - Always use disappearing messages, and before an action, reduce the time they take to disappear proportionally
  - Avoid putting your real name or details in your profile - choose an alias
- Email:
  - Use Protonmail https://protonmail.com/
  - **Definitely** avoid Gmail, Outlook, Hotmail etc.
  - Enable FaceID, TouchID, or PIN on the app
- Meetings:
  - Use Signal for up to 40 people
  - Otherwise, Zoom is okay IF END-TO-END ENCRYPTION IS ENABLED (this is not the default)

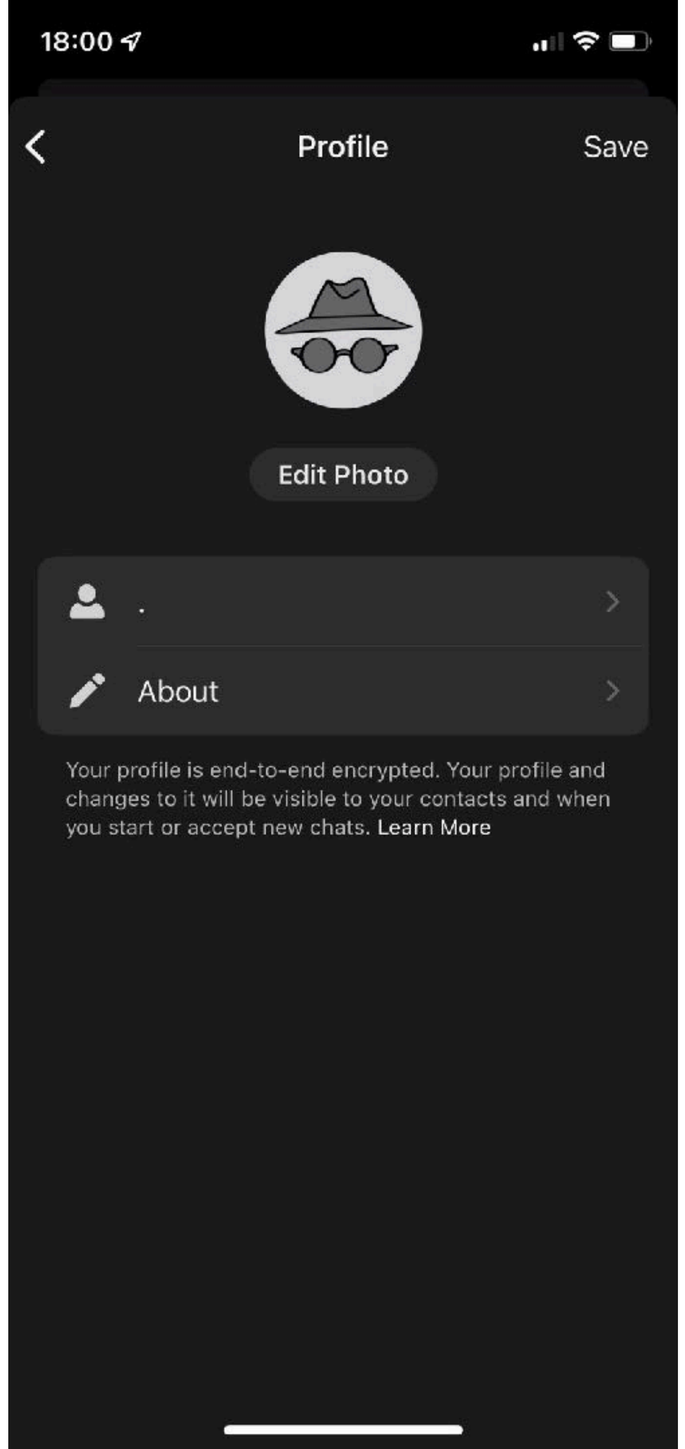
End-to-end encryption vs. encryption

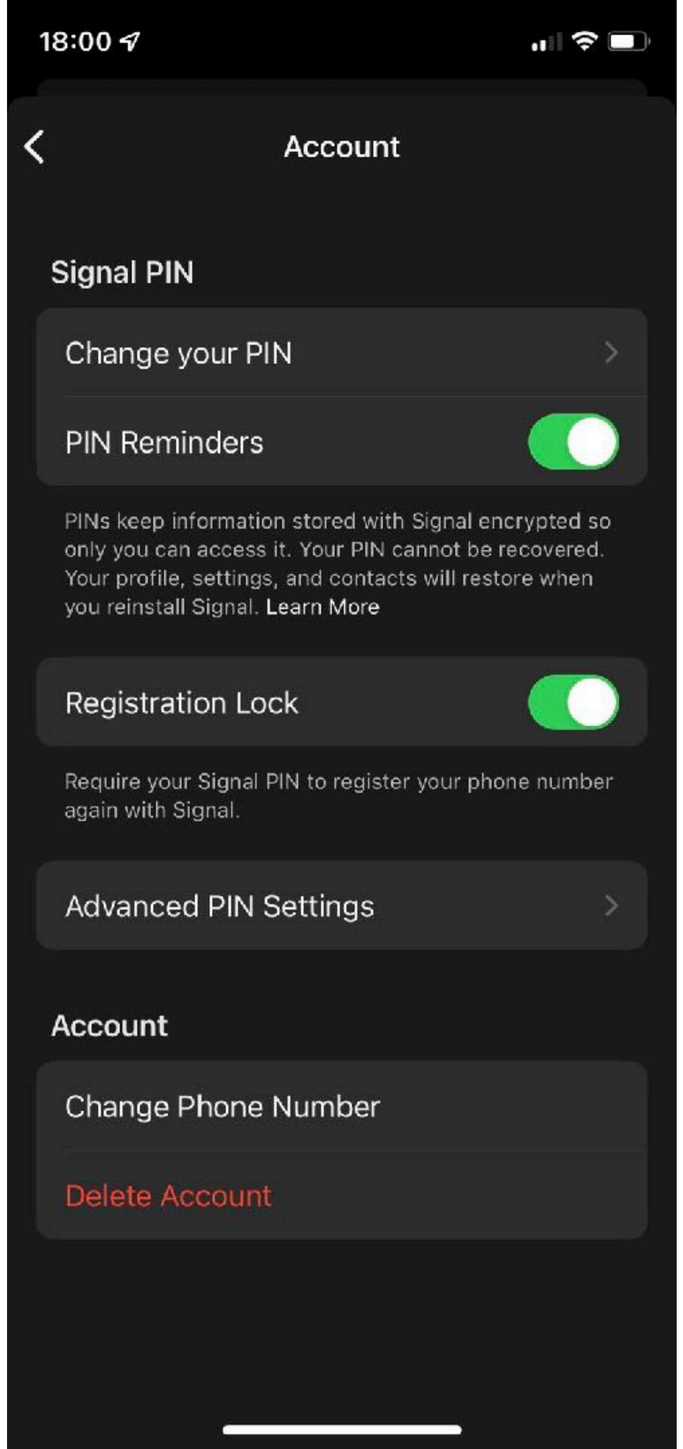
- **End-to-end** - only you and the other *end* users of the call or messages can read/see the content
  - If it doesn’t say end-to-end, it’s not end-to-end (e.g. Zoom’s default)
- **Not end-to-end** - the company running your chats or call can read/see the content and:
  - Watch/read it in real time
  - Record it for later
  - Send it to the police or government

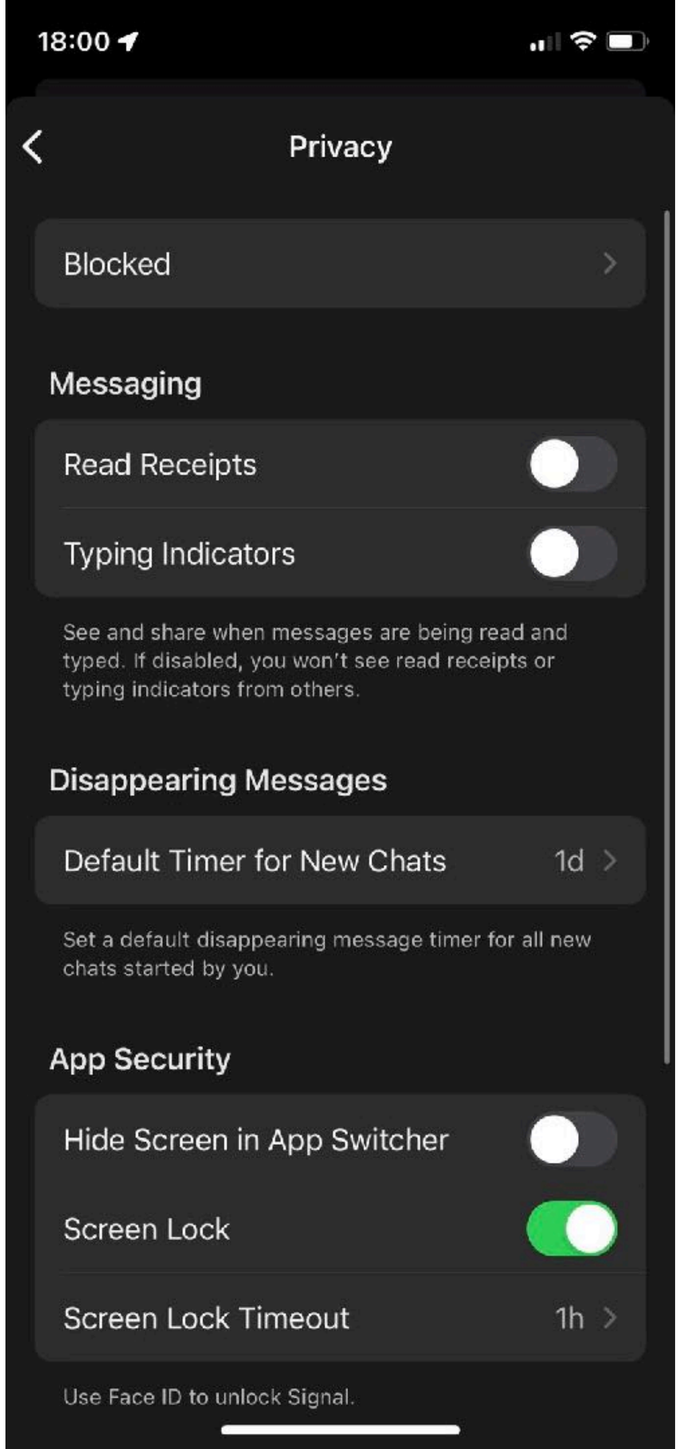
Important Signal settings

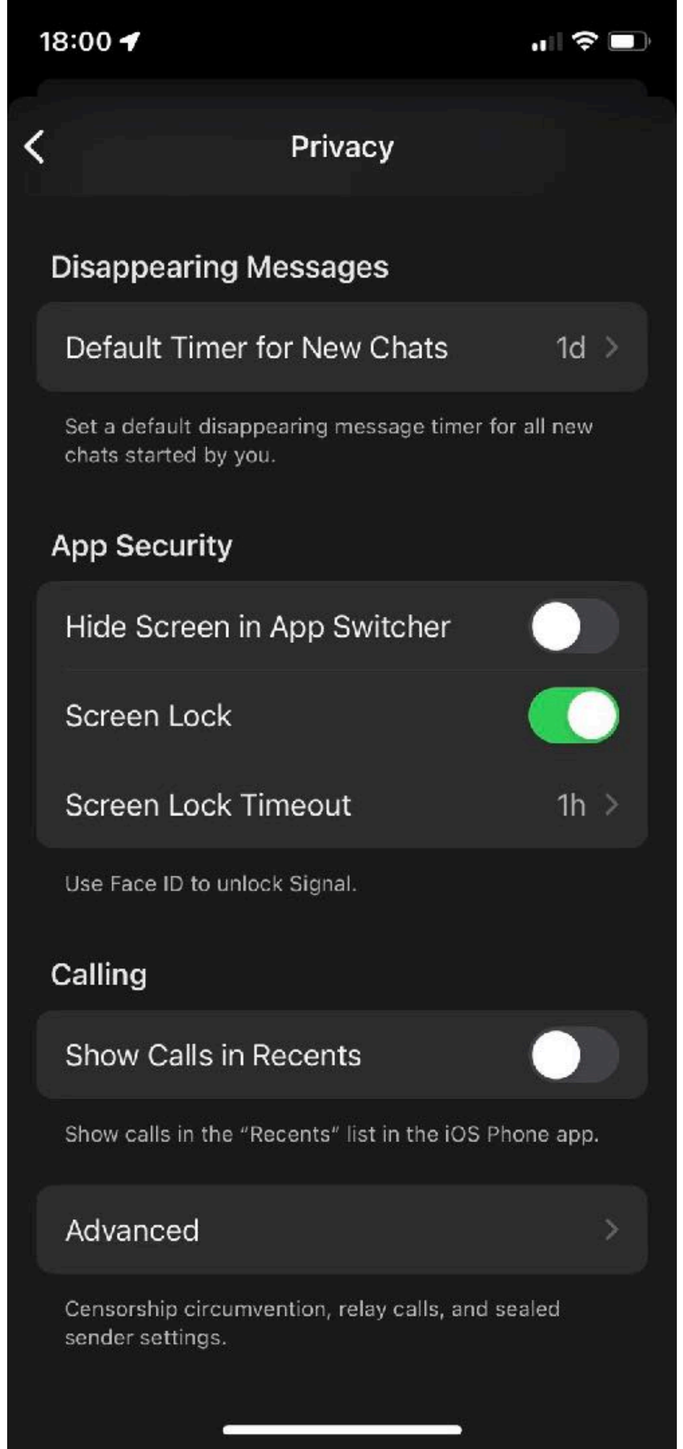
- Name and photo - use an alias and generic picture
- Account
  - Add a PIN and turn on PIN reminders
  - Turn on registration lock
- Privacy
  - Set default disappearing messages
  - Turn on screen lock
  - Don’t show calls in recents


18:00
Done
Settings
Account
Linked Devices
Payments
BETA
Appearance
Chats
Notifications
Privacy
Data Usage
Help
Invite Your Friends
Become a Signal Sustainer
Signal Boost


18:00
Profile
Save
Edit Photo
.
About
Your profile is end-to-end encrypted. Your profile and changes to it will be visible to your contacts and when you start or accept new chats. Learn More


18:00
Account
Signal PIN
Change your PIN
PIN Reminders
PINs keep information stored with Signal encrypted so only you can access it. Your PIN cannot be recovered. Your profile, settings, and contacts will restore when you reinstall Signal. Learn More
Registration Lock
Require your Signal PIN to register your phone number again with Signal.
Advanced PIN Settings
Account
Change Phone Number
Delete Account


18:00
Privacy
Blocked
Messaging
Read Receipts
Typing Indicators
See and share when messages are being read and typed. If disabled, you won't see read receipts or typing indicators from others.
Disappearing Messages
Default Timer for New Chats
1d
Set a default disappearing message timer for all new chats started by you.
App Security
Hide Screen in App Switcher
Screen Lock
Screen Lock Timeout
1h
Use Face ID to unlock Signal.


18:00
Privacy
Disappearing Messages
Default Timer for New Chats
1d
Set a default disappearing message timer for all new chats started by you.
App Security
Hide Screen in App Switcher
Screen Lock
Screen Lock Timeout
1h
Use Face ID to unlock Signal.
Calling
Show Calls in Recents
Show calls in the "Recents" list in the iOS Phone app.
Advanced
Censorship circumvention, relay calls, and sealed sender settings.

Using the internet

Using the internet - main points

For phone and computer

- Browser
  - **Definitely** don’t use Chrome or Edge
  - Use Brave browser https://brave.com/
  - Alternatively, Safari is okayish
- Use a VPN
- Use DuckDuckGo instead of Google for search http://duckduckgo.com
- Use a password manager (Apple has Keychain built in)
- Don’t use public or free wifi (without a VPN)
- Log out of Google and Microsoft in your apps

VPN

For phone and computer

- Hides your IP address (i.e. hides your physical location)
- Hides your internet activity from your service provider who **will** be logging and tracking you (they're surveillance capitalists now)
    - Your service provider is legally obliged to hand over data on what you've been doing when asked by the government/police
- Blocks malware, ads, and trackers
- Have Protonmail? Then you also have a ProtonVPN account
- https://protonvpn.com/

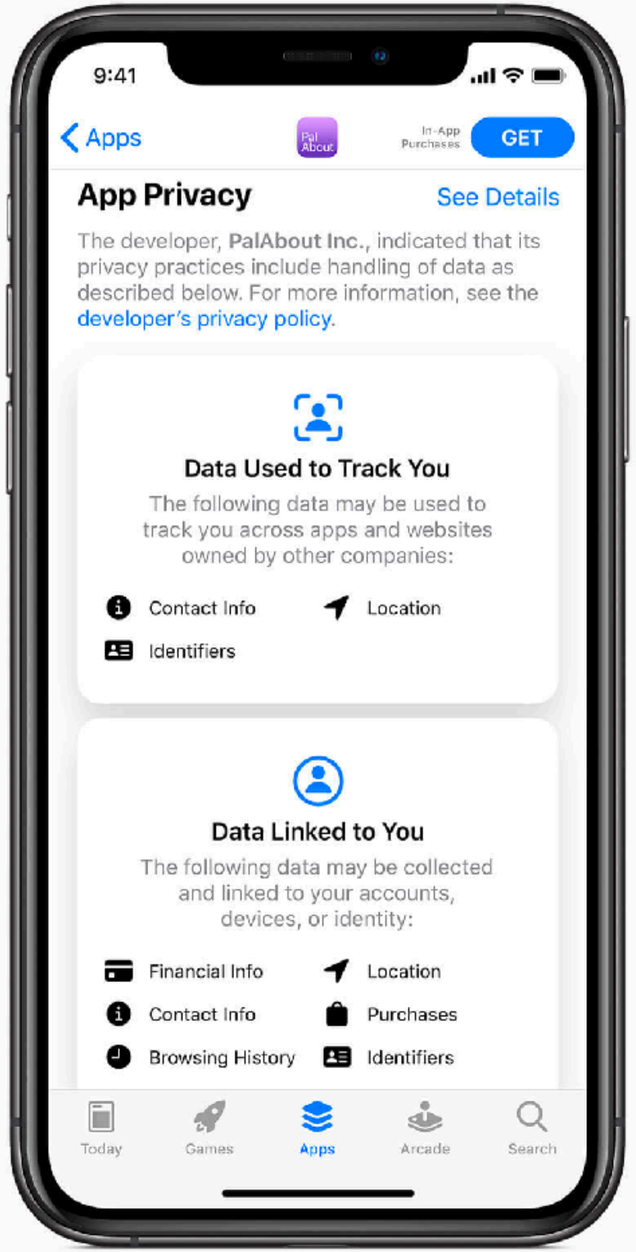
Online office and storage

- Use cryptpad.fr by default
- If you use Google Drive:
  - Set the privacy settings to maximum
  - Make it as anonymous as possible (e.g. make an account for your local group that you share)
  - Never store activists’ personal details
  - Never store spicy action details
  - Avoid using Google drive as much as possible

Phone security

Phone security - main points

- Encryption!! (doesn't work unless phone is turned off)
- Passcode **not** face or fingerprint; delete data on 10 failed attempts
- Don't show notification details unless unlocked
- Disable app tracking
- Limit access to location services and other personal things
- **Don't** use Google maps - use Apple maps
- Don't name your phone after yourself
- Disable targeted ads
- Avoid taking your phone to protests where you are likely to be arrested
- If you take your phone:
  - **Fully** turn off wifi and bluetooth at protests
  - Turn off your phone your phone when you can, and definitely before arrest



Main points continued

- Remove unused apps
- Always update your phone and apps

If your device is seized

- You are under no legal obligation to open it, no matter what they say to you. They will try and scare you in to opening it
- If you give them the passcode, they will have full access to your phone, potentially forever
- This puts all your activist friends at high risk of raids, arrest, and conviction

If your device is about to be seized

- If you have time, clear data on signal and delete the app
- If you don’t have time for this, just switch the phone off
- Try and hide the phone or give it to someone else
- Don’t respond to questions about where the phone is or may be - no comment

Computer security

Computer security - main points

- Encryption!! (doesn’t work unless computer is turned off)
- Require password immediately; don’t use biometrics
- Firewall
- Don’t name your laptop after yourself
- Limit access to location services and other personal things
- Don’t show notification details unless unlocked
- If using Safari, prevent cross-site tracking

Main points continued

- Remove unused apps
- Always update your phone and apps