Building a Social App on top of Matrix
Fighting surveillance capitalism for fun and profit

Charles V. Wright
Lead Software Engineer at FUTO
cvwright@futo.org

Matrix Dev Room
Brussels, 2023-02-05
Bio / Introduction

About me

👨🎓 Former CS professor
☢️ Security and privacy researcher
👪 Husband and dad

About FUTO

- Founded in 2021 by Eron Wolf, creator of Yahoo! Games

- Mission:
  - Empower users
  - Reduce reliance on tech giants
# Motivation

How to securely ... share baby photos ???

<table>
<thead>
<tr>
<th></th>
<th>Cross Platform</th>
<th>Private</th>
<th>Async Convenience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Photos</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>Apple Photos (iCloud)</td>
<td>✗</td>
<td>?</td>
<td>✔</td>
</tr>
<tr>
<td>Facebook / Instagram</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>Photobucket / Shutterfly / etc</td>
<td>Web</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>Signal etc (Matrix, Wire, Wickr, Threema, ...)</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
</tr>
</tbody>
</table>
## Motivation

How to securely ... share vacation photos ???

<table>
<thead>
<tr>
<th></th>
<th>Cross Platform</th>
<th>Private</th>
<th>Async Convenience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Photos</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>Apple Photos (iCloud)</td>
<td>✗</td>
<td>？</td>
<td>✔</td>
</tr>
<tr>
<td>Facebook / Instagram</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>Photobucket / Shutterfly / etc</td>
<td>Web</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>Signal etc (Matrix, Wire, Wickr, Threema, ...)</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
</tr>
</tbody>
</table>
### Motivation

How to securely ... run an online book club???

<table>
<thead>
<tr>
<th></th>
<th>Cross Platform</th>
<th>Private</th>
<th>Async Convenience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Photos</td>
<td>❌</td>
<td>❌</td>
<td>✔</td>
</tr>
<tr>
<td>Apple Photos (iCloud)</td>
<td>❌</td>
<td>?</td>
<td>✔</td>
</tr>
<tr>
<td>Facebook / Instagram</td>
<td>✔</td>
<td>❌</td>
<td>✔</td>
</tr>
<tr>
<td>Photobucket / Shutterfly / etc</td>
<td>Web</td>
<td>❌</td>
<td>✔</td>
</tr>
<tr>
<td>Signal etc (Matrix, Wire, Wickr, Threema, ...)</td>
<td>✔</td>
<td>✔</td>
<td>❌</td>
</tr>
</tbody>
</table>
Motivation

How to securely ... share baby photos ???

<table>
<thead>
<tr>
<th></th>
<th>Cross Platform</th>
<th>Private</th>
<th>Async Convenience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Photos</td>
<td>❌</td>
<td>❌</td>
<td>✔</td>
</tr>
<tr>
<td>Apple Photos (iCloud)</td>
<td>❌</td>
<td>?</td>
<td>✔</td>
</tr>
<tr>
<td>Facebook / Instagram</td>
<td>✔</td>
<td>❌</td>
<td>✔</td>
</tr>
<tr>
<td>Photobucket / Shutterfly / etc</td>
<td>Web</td>
<td>❌</td>
<td>✔</td>
</tr>
<tr>
<td>Signal etc (Matrix, Wire, Wickr, Threema, ...)</td>
<td>✔</td>
<td>✔</td>
<td>❌</td>
</tr>
</tbody>
</table>
Goals

1. Most of the convenience of Facebook
   • Read: Easily keep up with a few hundred people
   • Write: Easily publish updates for all your friends to see
   • Explicitly asynchronous

2. Most of the security and privacy of Signal
   • Confidentiality: Servers can’t spy on your messages
   • Integrity: Servers can’t inject junk into your timeline

3. Freedom from Big Tech megacorps
   • Independence: Users can run their own servers
High-Level Goal: Social Networking

Focus on enabling real human relationships between real people

Facebook has become a ghost town
(See the “Dead Internet Theory”)

Normal families are stuck using SMS and email like it’s 2003
- Social network in the front
  - Easy
  - Convenient
  - Familiar
- Matrix in the back
  - Encrypted
  - Federated
  - Open standards
  - Open source
Challenges

• **Challenge 1: Mapping human social structures onto Matrix**
  - Groups
  - Friends

• **Challenge 2: Balancing privacy and ease of use**
  - Discoverability vs Privacy
  - Making SSSS easier for users
Challenges

• Challenge 1: Mapping human social structures onto Matrix
  • Groups
  • Friends

Focus of this talk

• Challenge 2: Balancing privacy and ease of use
  • Discoverability vs Privacy
  • Making SSSS easier for users
Social Structures

Friendships and similar relationships

- Flexible, harder to define
- Asymmetric — Not everyone is connected in the same ways

Groups

- Well-defined membership
- Everyone is connected to each other
Social Structures: Private Groups

Mapping this structure onto Matrix: Easy Mode

Insight: It’s just a chat room with a different (async / social) UI!

Solution: Create one Matrix room for the whole group
Social Structures: Private Groups

Easy mode: One timeline, One room

All posts for the group go into the same Matrix room
Social Structures: Private Groups

Easy mode: One timeline, One room

All posts for the group go into the same Matrix room

Client renders the events as “social” posts
Social Structures: Secure Social Circles
Mapping human connections onto Matrix rooms

• Challenge: Friend relationship structures are asymmetric, non-transitive
Social Structures: Secure Social Circles
Mapping human connections onto Matrix rooms

- Insight: DON’T PUT EVERYONE INTO THE SAME ROOM!
Social Structures: Secure Social Circles
Mapping human connections onto Matrix rooms

• Your friends want to see updates from you — They go in one room
Social Structures: Secure Social Circles
Mapping human connections onto Matrix rooms

- My friends want to see updates from me — They go in a different room
Social Structures: Secure Social Circles
Mapping human connections onto Matrix rooms

• Our mutual friends should be members of both rooms
Social Structures: Secure Social Circles
Mapping human connections onto Matrix rooms

- Solution: Create one Matrix room for each person
  - Owner posts their updates in the room
  - Other users (“followers”) mostly only read *

*One common exception to the rule: Posting “Happy Birthday!!” in a friend’s room*
Social Structures: Secure Social Circles
Mapping human connections onto Matrix rooms

Client fetches and collates events from all of your friends’ rooms
Social Structures: Secure Social Circles

Collating timelines

Client renders one unified chronological timeline
Social Structures: Secure Social Circles

Collating timelines

Bonus: You’re not limited to a single circle of friends
FUTO Circles on iOS
Beta is paused while we re-write the SDK... Coming back soon!
FUTO Circles for Android
Now in beta on Google Play and in our F-Droid repo

Circles beta repo

Beta releases of the Circles app.
Currently it serves 1 apps. To add it to your F-Droid client, scan the QR code (click it to enlarge) or use this URL:

https://circu.li/fdroid/repo

If you would like to manually verify the fingerprint (SHA-256) of the repository signing key, here it is:

BD BD CD 45 6A DC DA F1 14 51 BF 90 E8 05 AF DB 2D 8D 76 CF 89 70 55 3F D9 6A 47 4B BE 08 EC 58
Android Screenshots
Future Work

New features in progress

• Profiles as spaces — Making discoverability easier
• Notifications

Plans for 2023

• Another round of public beta test on Android and iOS
• Support for MSC3917: Cryptographically Constrained Room Membership
• In-app subscriptions via Google and Apple — Hosted accounts for a few $/mo
• Production release on both platforms
• Growth! 🚀
Thanks!
Follow the project:  #circles:matrix.org

Get the code:
https://gitlab.futo.org/circles/circles-ios
https://gitlab.futo.org/circles/circles-android

Try the Android beta: