Revocable Privacy

Privacy Seminar

Anushka, Sam & Ysbrand

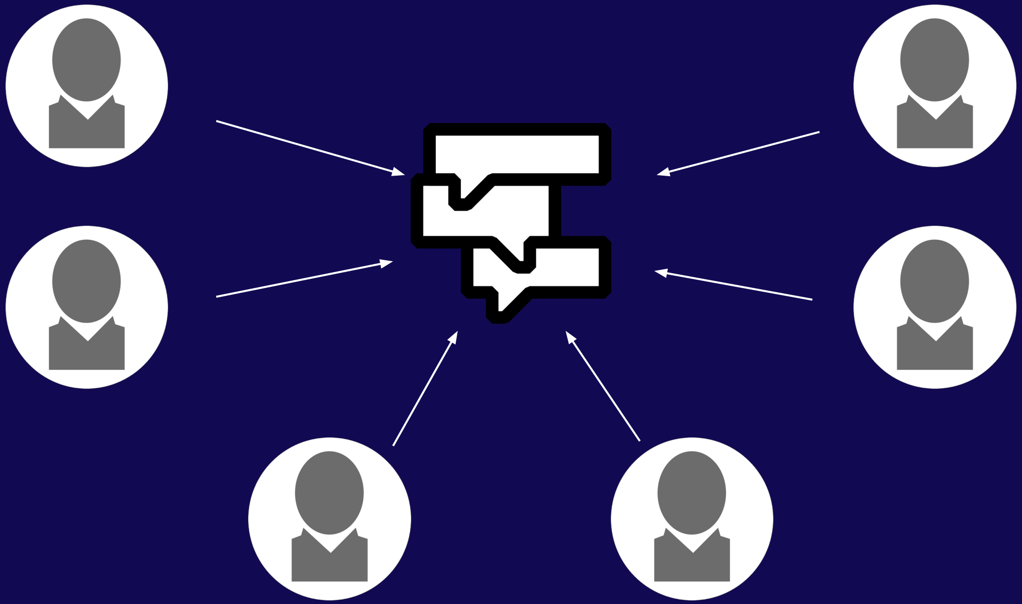
Table of Contents

- Definition
- Bytes of Freedom
- Different designs
- Technical implementation
- Ethical aspects
- Legal aspects
- Rounding up

Definition

<Revocable>Privacy<Revocable/>

Bytes of Freedom



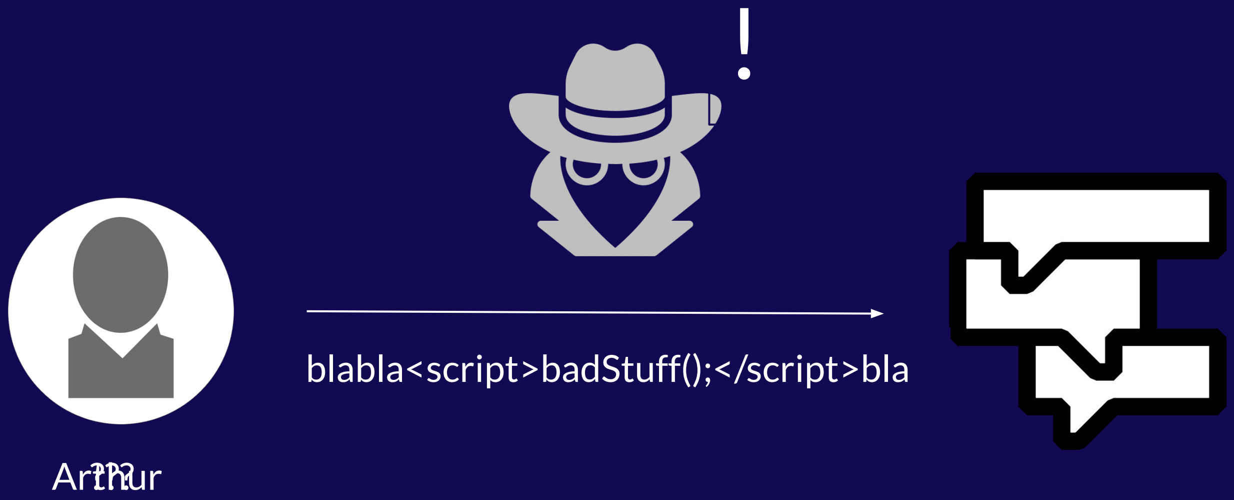
Registration

Hello, Arthur

<name> Arthur
<age> 28
<email> arthur911@gmail.com
…

Logging In

Conceptually



!

blabla<script>badStuff();</script>bla

Arthur

???

Revocable Privacy on BoF

<Revocable>Privacy<Revocable/>

Hateful Speech

Requirements:

-No immediate revoke of privacy

-No continuous hate speech

Resources:

-Wordlist

Threshold Rules

<Rule>No more than 50 matches with the words in de wordlist within a day.</Rule>

Malicious JavaScript

Requirements:

-Immediate flag and revoke of privacy

Resources:

-Function logging

Predicate Rules

<Rule>Occurrence of “<script>”/\ JavaScript function executed /\ call to external not-listed domain.</Rule>

Selling Drugs

Requirements:

-The sellers should be identified

-Clear and vague language should be spotted

Resources:

-Post history of a discussion or user

Decision Rules

- <Rule>If n moderators deem the conversation as a form of drug selling, the identity of the participant is revealed.</Rule>

Hacked User

Requirements:

-Hacked users should be identified

Resources:

-...

Complex Rules

- <Rule> If a user suddenly switches completely in interests /\ the recovery mail of the user has been changed in the last week, the privacy is revoked.</Rule>

Different Designs

- Threshold rules (hateful speech)
- Predicate rules (malicious JavaScript)
- Decision rules (selling drugs)
- Complex rules (hacked user)

Technical Implementation

How to implement these things on a technical level?

Hateful Speech

- Back to the Hateful Speech example
- Have: wordlist and some reports of hateful speech
- We could use threshold decryption to implement this
  - Note that this may not be the bestest of use-cases, but or the sake of staying with the example it suffices.

- We'll be using the Shamir's Secret Sharing scheme
  - Though there are other schemes that we could've used instead, like:
    - Blakley's scheme
    - Feldman's scheme (which is, in turn, based on Shamir's)
    - Secure Multiparty Computation
      - Which is more of a generic catch-all

Intermezzo: Shamir's Secret Sharing

Intermezzo:
Shamir's Secret Sharing

A secret sharing algorithm.

Have:

- Some private information ('the secret')
- A group of (m) parties
- Some threshold value (the 'quorum') (n; n <= m)
    - (We'll get back to this soon!)

Intermezzo:
Shamir's Secret Sharing

- The secret is divided into m 'shares'
- Each party gets a share
- On their own, a party can not reassemble the secret
    - In fact; the quorum number of shares are needed for reassembly

Intermezzo: Shamir's Secret Sharing

Some use-cases:

- Sharing a key with which a root key of sorts is encrypted
- Recovering user keys for email access
- Passphrase encryption for crypto wallets
- And, of course; Bytes of Freedom!
    - To which we'll back to in a bit. Hang tight!

Intermezzo:
Shamir's Secret Sharing

The good:

- Secure
- Minimal
- Extensible
- Dynamic
- Flexible

Intermezzo: Shamir's Secret Sharing

The a-bit-less-good:

- No verifiable secret sharing
  - Feldman's -which we mentioned earlier- *is* a VSS scheme
- Single point of failure

Intermezzo:
Shamir's Secret Sharing

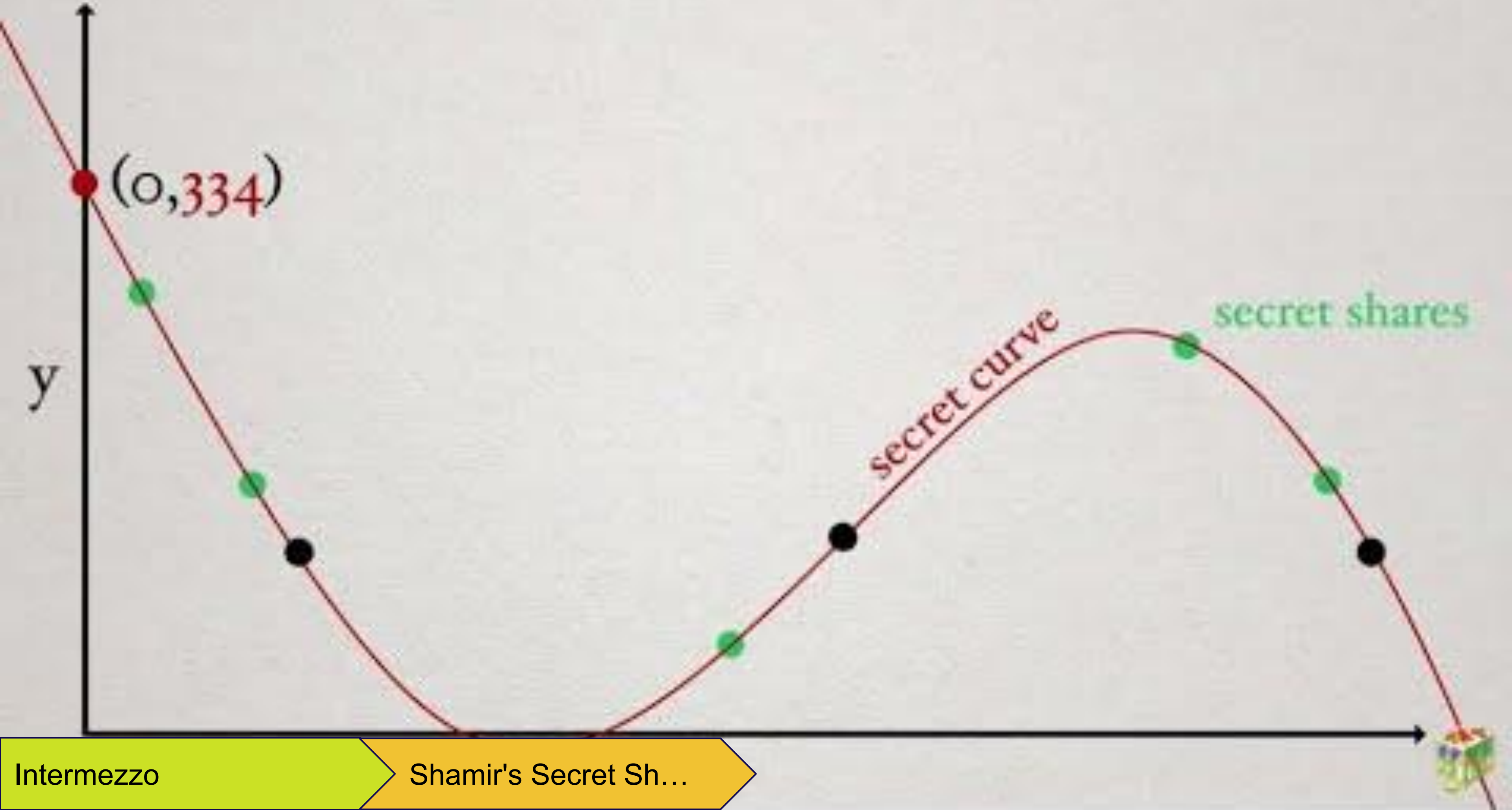
How do we make and merge these shares?

- MATHS!

(Well, kind of. More like "maths".)

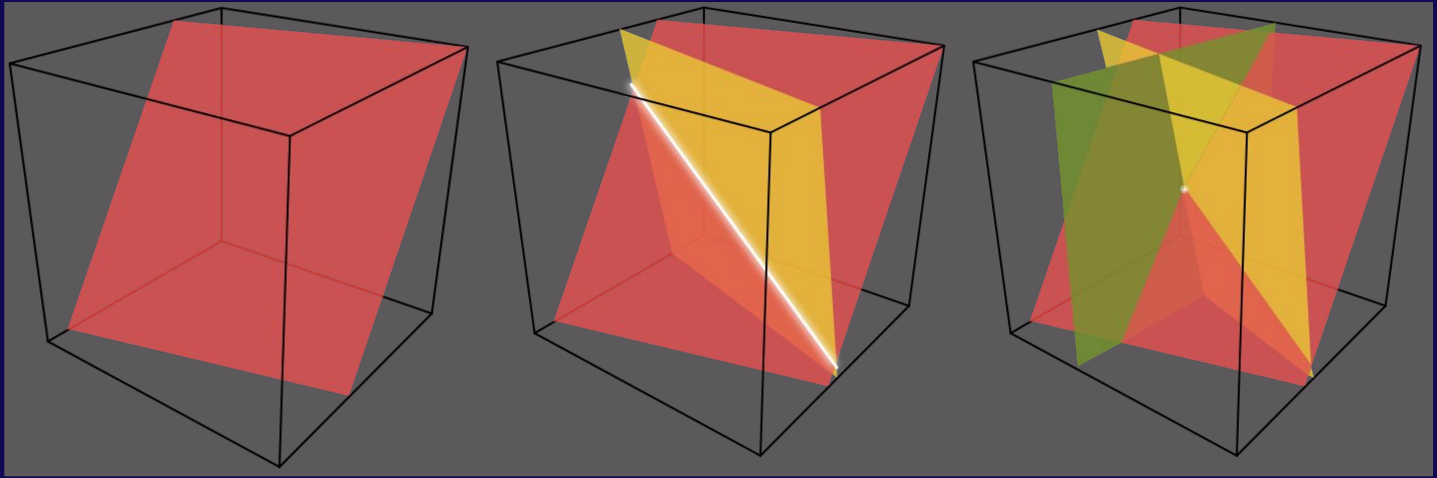
Intermezzo:
Shamir's Secret Sharing

- Say we want to 2 out of 3 shares be able to reassemble
- t = 2, n = 3
- With 2 (t) points, we can define a polynomial of degree 1 (t-1)
- Secret: 1st coefficient; remaining are random
- Find n points on the curve and give one to each holder
- To fit the polynomial, you need t out of n points; the first being the secret


(0,334)
y
secret curve
secret shares

Intermezzo:
Shamir's Secret Sharing

As an aside: Blakley's scheme works roughly the same but with planes:



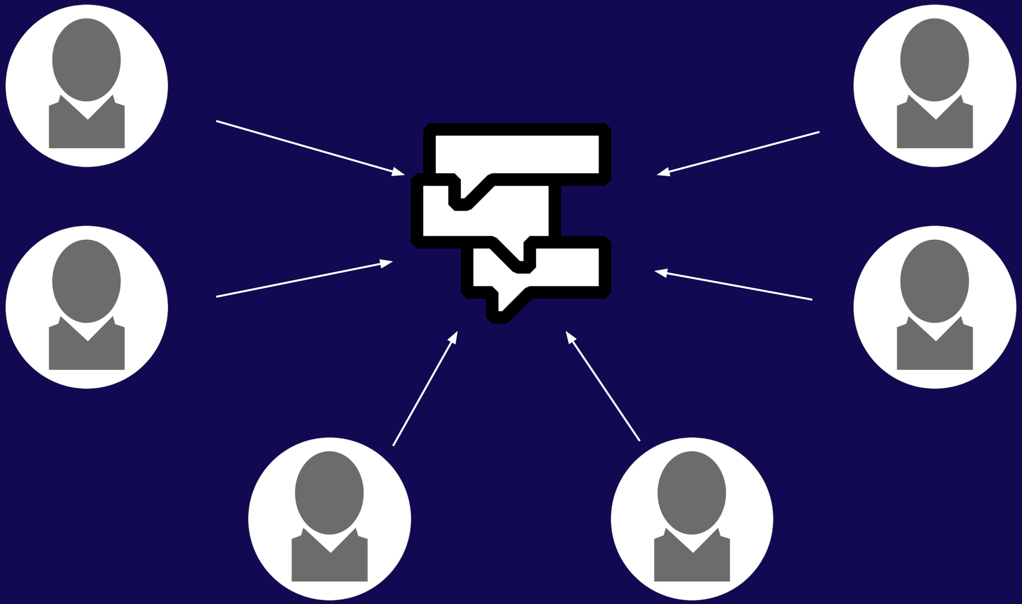
Intermezzo: Shamir's Secret Sharing

There's a toy code-example on Wikipedia:

https://en.wikipedia.org/wiki/Shamir%27s_secret_sharing

But enough maths for now.

Bytes of Freedom



Hateful Speech

Upon registration:

- Personal information is encrypted ('the secret')
    - Things like email address or phone number
    - In this context we call these 'revocable attributes'
- The secret is divided into shares

Hateful Speech

Upon posting on the forums:

- The message is checked against the wordlist
- For each match, a share is released
- With enough shares released, the moderators can reconstruct the personal information of the user

Selling Drugs

- Back to another example: Selling Drugs

- Some very bad actors; how to ban?
- Recall: users have a private key; not a user+pass
    - They use the private key to generate a random token each time they login
- For this we can use a thing called "blacklistable anonymous credentials"

Time for another intermezzo!

Intermezzo: Blacklistable Anonymous Credentials

Intermezzo: Blacklistable Anonymous Credentials

A system for allowing anonymous logins, whilst maintaining the ability to ban users.

- Have:
  - A service (like, say, a forum)
    - And sometimes: a separate verifier
  - Some users who want to use the service anonymously
  - Providers of the service who might want to ban users

Intermezzo:
Blacklistable Anonymous Credentials

- Service initializes backlist to an empty list
- Users get their private key during registration

Intermezzo: Blacklistable Anonymous Credentials

- Multiple possible implementations
- We'll be using NTAC:
  Non-Transferable Anonymous Credentials

In this system:

- Keys can not be linked back to users
- Keys are meant to not be transferred to another user

Intermezzo: Blacklistable Anonymous Credentials

Upon logging in:

- User submits their key to the verifier
- The verifier compares the key against all tokens on the blacklist
    - More on this soon
- …

Intermezzo:
Blacklistable Anonymous Credentials

- ...
- If none of the tokens on the blacklist belong to the user they get a new token to login with on the service
- Otherwise, they don't

Note that the token that they get can not be linked to the other tokens generated by the same key, without the key.

Intermezzo: Blacklistable Anonymous Credentials

The service can ban/blacklist a user by simply adding their current token to the blacklist and revoking their current session.

Intermezzo: Blacklistable Anonymous Credentials

Getting back to the verifier:

- One way would be to append a salted hash of the key to the token
  - So basically {random value,hash of(private key|random value)}
- However; zero-knowledge proofs are used in the paper
  - But I'm not smart enough to be able to explain those. Sorry!

Intermezzo:
Blacklistable Anonymous Credentials

The good:

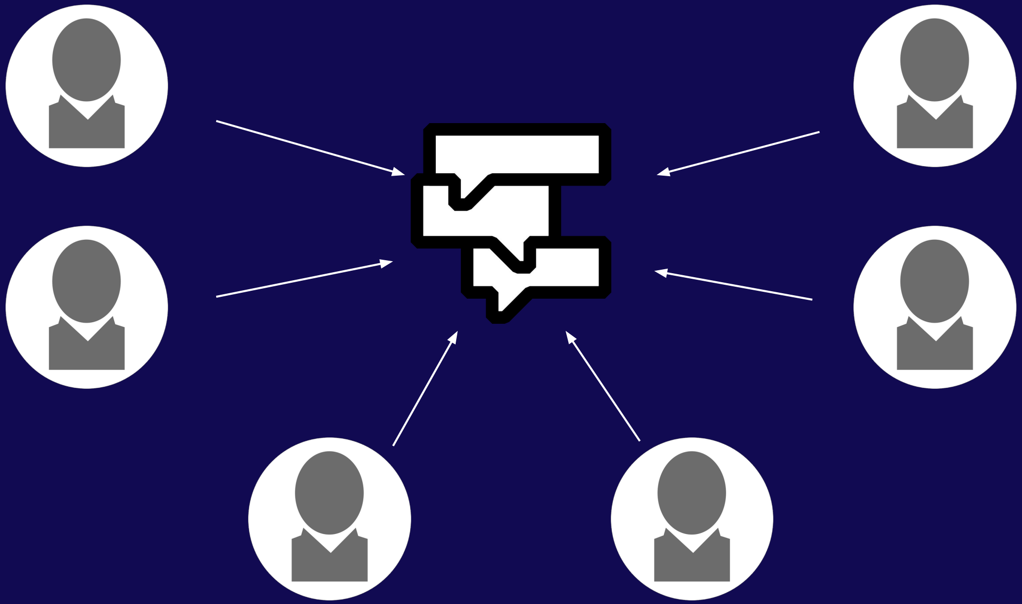
- Tokens can be removed from blacklist
  - Useful for temporary bans
- Allows for banning a user after they've been put on the list x times

Intermezzo:
Blacklistable Anonymous Credentials

The a-bit-less-good:

- Time complexity, mainly. Logging in is linear to the number of tokens on the blacklist.

Bytes of Freedom



Selling Drugs

- The same as in the generic, non-BoF, example. ;-)

Technical Implementation

- Threshold decryption
  - Which is a subcategory of "distributed decryption"
- Blacklistable anonymous credentials

But also so much we haven't been able to discuss:

- N-times anonymous encryption
- Group signatures with distributed management
- Secure multi-party computation

(Maybe when we have a bit of time left)

Privacy enemy <or> Privacy saver

- Moderator
- Eve
- Secret services

Ethical Issues

- Misuse of anonymity
- Accountability
- Privacy violation
- Decision-making

Ethical Aspects

- False Positives
- False Accusations

False Positives

When a system or algorithm mistakenly classifies or categorizes a behaviour as a risk.

False Positives

1. Imperfect algorithm
2. Incomplete information
3. complexity of data analysis

Examples

1. Accidental wiretap
2. Misclassification of activities
3. False alarms

False Accusations

claims or allegations made against individual which can incorrect or baseless

the consequences an individual can face as a result of incorrect/unjust claims

False Accusations

1. Personal information
2. Reputation
3. Legal remedies
4. Accountability

Examples

- Cyber bullying
- Sexual misconduct
- Child abuse

Legal Aspects

Legal frameworks that enforce revocable right

- Short-lived laws
- Data privacy laws

Short-lived laws

- Escrowed Encryption Standard Initiative
- EU Data Retention Directive

Data Privacy Laws

1. GDPR
2. California Consumer and Privacy Act

Privacy vs Revocable Privacy

Advantages

- control
- flexibility
- time limited access
- transparency

Disadvantages

- complexity
- limited scope
- potential for abuse
- inconvenience

Rounding Up

Recap

1. Definition
2. Different designs
3. Technical implementation
4. Ethical aspects
5. Legal aspects

//?

Other Places for Revocable Privacy

Recent News

- Apple's CSAM detection

Discussion