Structure of Z's proposal

What do they want to do?

- offer a living room compared to the current town square
- privacy-focused messaging
- follow trends of people wanting fewer permanent records and more intimate conversations
- give users the confidence that they have control over who receives their messages
- messages and calls are some of the most private things, so they must be protected
- unify their services

How will they do that?

- working together is needed to get this right
- only store data in secure locations

1. Encryption
   - secure communications so that no one else can access them
   - use e2e encryption on all services like on WhatsApp right now
   - this protects from hackers, overreaching governments and service providers
   - fewer people with access means fewer chances of a breach
   - e2ee is central to this – decentralizes as no one can read the messages
   - even if data is at rest, the encrypted form is pretty useless
   - even with all the drawbacks, Z thinks e2ee is the way to go
2. Reduced Permanence
   - people can be hurt or inconvenienced by old content
   - data should only be stored as long as needed or desired
   - people could set times for data to expire or have it do that automatically
   - lots of data is an asset and a liability at the same time
   - meta data too should be stored for shorter periods of time – it's only needed for spam and safety filters
   - collecting less information in the first place

Issues

- keeping people safe on an encrypted service as best as they can, but that can be hard as they cannot read the messages or data
- data needs to be stored in places where it is safe from abuses of the law
- people need to trust the data storage in order to be able to trust the service
- is a tradeoff between safety and security
- encryption includes privacy to do bad things: cse, terrorism, extortion
- FB has to work with LEAs to do the best they can
- encryption makes checking more difficult than it even is today