Privacy-Focused Vision for Social Networking

Introduction

- Z was addressing the biggest challenges facing FB
- means taking positions concerning the future of the internet
- he'll outline visions and principles around a privacy-focused messaging and social networking platform
- last 15 years: helping people connect with friends in kind of a town square
- now they also want to be a living room
- privacy-focused communications will be more important in the future
- privacy gives people the freedom to be themselves and connect more naturally
- we see private messaging, ephemeral stories, small groups are the fastest growing area of online communications
- intimacy is often important: one-on-one or with few friends
- permanent records are less liked now
- everyone expects to be able to do stuff privately
- public sm will remain important – there is still a lot of value there – but now there is an opportunity to build a simpler, privacy focused platform
- he knows most people would not expect FB to do something like this, they do not currently have a good reputation for that
- but they have also shown that they can respond to demands and build private stories or messaging
- Z believes comms will become more private, encrypted services – messages are secure and not around forever
- building shall be like WhatsApp: messaging, as secure as possible, and then build stuff on top of that

Private interactions

- simple, intimate places with clear control over who can communicate and have security that no one can access stuff

Encryption

- private communication should be secure – end-to-end encryption does that and prevents anyone from reading them

Reducing Permanence

- people should be themselves without worrying that stuff comes back to hurt them
- messages won't be around longer than necessary for delivery or how long the user wants

Safety

- do all that they can to keep people safe on an encrypted service

Interoperability

- any of their apps should be able to communicate with all others across networks and securely do so

Secure data storage

- not storing data in countries with weak records of human rights (privacy, freedom of expression) to prevent improper access

Recap

- over the next few years they want to build more of their services around these principles
- there are a lot of tradeoffs to get right, and they will do the best and consult experts and out in the open

Private Interactions as a Foundation

- privacy = never any doubt about who are you communicating with
- public networks have their uses for all kinds of stuff – more like a town square than a private group
- there is the opportunity to build a social network that is more like a private living room
- making a service *feel* private is much more than the tech behind it – it involves design that gives the user the feeling of privacy too
- Z expects Messenger and WhatsApp to become the main ways people communicate on the FB network
- focused on making both of these apps faster, simpler and more secure **including entd-to-end encryption**
- then they'll add more features that allow private communications
- this will make everything easier and more private

Encryption and Safety

- private communications should be only seen by the intended recipients and not hackers, **over-reaching govs** or even the service operators
- growing awareness of the relation between the number of actors and the likelihood that an error or attack would expose the data
- technology can be seen as centralizing power in the hands of some governments or companies; or accessing data for advertisements and the like
- **e2e encryption is an important tool in developing of privacy-focused networks**
- encryption is decentralizing – it takes power away from central authorities that now cannot read the messages – **that is why the built e2e into WhatsApp**
- encryption can help dissidents and keep them alive
- if a gov asks for data outside of legality but it's enforced, if there is no encryption, FB would have to expose plain text data
- all the same, there are a lot of problems to solve before e2ee can be implemented across all the services
  - encryption includes the privacy to do bad things
  - some of users will do horrible things with their privacy: child exploitation, terrorism, extortion
  - FB has the responsibility to work with LEAs to do whatever they can
  - there will be a definite tradeoff, as even today when they can see the messages some slip through the cracks – encrypted this would be even more difficult
  - there are still many questions related to that and they will consult with experts, LEA and govs on ways to implement safety measures
  - we need to work together to get this right
- on balance, implementing e2ee is the right thing to do
- messages and calls are some of the most private conversations people have so they are worth protecting in this dangerous world
- we'll take all possible steps to stop bad actors withing the confines of an encrypted service
- WhatsApp is a stepping stone in this picture; there has to be more discussion

Reducing Permanence

- information should be around for shorter periods of time
- people don't want to be bitten in the ass by stuff they shared, so reducing the amount of time information is stored will help with that
- over time large amounts of data build up and this is an asset and a liability at the same time
- so content could be set to automatically expire over time like in Stories after 24h – people can now share more naturally
- default deletion time could be 1 month or one year, reducing the risk of messages resurfacing; could of course be turned off or set to seconds or minutes for certain messages
- length of time that messaging metadata is stored should also be reduced – it's used for spam and safety systems, but they don't need it for a long time
- important part of the solution is to collect less personal information in the first place, WhatsApp was built like this from the start

Interoperability

- you should be able to use the messaging service of your choice to communicate with all people on the other services without issues
- they want to start by allowing people to send messages to their contacts using any of the services, later SMS too – would be opt-in so you can separate your accounts too
- this has privacy and security advantages: instead of unencrypted SMS through messenger, you could send a WhatsApp message from messenger to that person's WhatsApp
- it would be easier as you don't have three different ways to message people, e.g. when selling stuff and giving your phone number – after this you wouldn't have to, as they could message you and you'd get a WhatsApp message instead
- some problems:
  - Apple does not allow SMS access from other apps so it's Android only
  - interoperability should not compromise existing encryption on WA
  - unknown apps could be used to send spam and stuff and compromise security
- there are many unsolved problems, but the end goal would be convenient and cool

Secure Data Storage

- the physical location of data is important as people need to trust them – the location of data centers is important
- providing services in a country != storing data there
- storing data in countries with a record of violating freedom of expression and the like would make it easy for that state to steal some data
- this means that their services will get blocked in some countries or never even be allowed in others, but that's ok
- not storing any important information is of course the way to go – **WhatsApp does not store any keys** and they want to design their other services the same way
- data should only be stored in places where it is secure

Next Steps

- there is still a lot of work to be done on these principles – we'll work with industry, experts, advocates, govs to get it right
- then there are more questions of what to build on top of that foundation
- the initial steps are the most crucial ones though
- as such we need to take positions on some of the most important issues of the internet
- I believe in a world where people can speak privately and live freely knowing that their information will only be seen by those who they want to see it and that it won't be around forever