Contents

Facebook Messenger – A Threat to Public Safety?

Introduction

Hook - Facebook Statement

Facebook proposes common-sense privacy goals for their messaging services – encryption and reduced permanence

- In May Mark Zuckerberg announced that Facebook Messenger would become more secure in the future. Facebook plans to implement secure encryption into its private messaging service to . . .
- short description of the note – **give the two main principles**
- this proposal seems very sensible, especially in a time where Facebook is not known for protecting privacy, as Mark Zuckerberg remarks in a self-aware way.

Source: Facebook Note

EU connection

The European Commission holds encryption to be highly important to digital infrastructure and fundamental rights

- The EU also sees this importance, they see encryption as a vital tool for everything that is important.
- state the importance of encryption here: online banking, private messaging, cloud data storage, online shopping
- Still, not everyone agrees that encryption and Facebook's proposals are a good idea

Source: 11th progress report of the EU Commission

Counter Statement

US, UK, Australian governments hold that encryption – especially on Facebook Messenger – can be a threat to public safety if it stops LEA from doing their jobs

- The ministers of the US, UK, and Australia wrote an open letter to Facebook and Mark Zuckerberg urging them not to go forward with their plans outlined in the note.
- concern over criminals evading LEA, *think of the children*
- the main idea is that privacy should not be put above security

Source: Open Letter to Facebook

EU connection

EU organizations like Europol and national LEA see encryption as a tool used by bad actors – mostly terrorists – to commit or organize their crimes

- how is this different from the open letter approach
- Even though the European Commission hails encryption, some other bodies of the EU are not so enthusiastic. Europol sees encryption as one of the major threats to their counter-terrorism work.
- give counter points that were made by EU institutions
- the EU political discussion is mostly concerned with encryption as a tool for terrorists

Source: 11th progress report, Encryption Debate Paper

Summary and Research Question

Why is encryption so important and devisive?

- it is both a huge asset and liability at the same time
- within the EU there is no concrete consensus on the issue
- questions that need to answered:
  - What is encryption and what is the general debate about?
  - What exactly is Facebook proposing and why is it a problem for LEA?
  - Contrasting the EU approach with the Open Letter approach
  - Is there a way to find a European solution?

Body

What is encryption and what is the general debate about?

What is encryption?

Encryption is the act of making data unreadable to outsiders – allows secure and confidential communications

- Encryption is putting data in code, make messages unreadable for potential snoopers
- **reiterate why it is important**
- example of % of people using the [internet graph][1] and/or internet usage for sm europe
- use the OECD guidelines and examples/explanations
- Encryption allows data to be privately and securely transmitted globally.

Source: OECD guidelines

General Issue

LEA want access to data to do their jobs – if that data is encrypted, they have a hard time doing their jobs

- what is *exceptional access*
- LEA want access to data, if they don't have it they fear that they cannot do their job correctly
- They want exceptional access to data
- One of the main issues in the EU is terrorism while in the US and UK it's cse
- how much citizens see terrorism as a problem open data cyber security
- these are valid concerns, but how do they want to do it?

Sources: IOCTA, Keys Under Doormats, Encryption Debate, 11th report

Methods of exceptional access

Exceptional Access of LEA – historically – can be facilitated through backdoors or weak encryption

- encryption is being used, so they have to deal with that somehow
- mention the Crypto Wars in passing
- backdoors are the storing of keys with third parties that can then be retrieved when LEA needs them – more precisely called key-escrow
- has the issue of organization, security principles, one big target for attacks
- the other is weak encryption – stuff that is easy to break – meaning that LEA does not need to get a key, they can just crack it

Sources: Keys Under Doormats

What exactly is Facebook proposing and why is it a problem for LEA?

Encryption and Reduced Permanence

Facebook wants to make private messages e2e encrypted and reduce the time that the message data is stored to increase privacy

- this is supposed to increase the feeling of a living room vs the current town hall
- they see a trend and shifting public opinion on data storage and big groups
- peoples opinions on privacy focused networks/fear of public exposure/trustworthy networks from barometers
- Mark acknowledges the problems this might have, but thinks that it's still the way to go
- connect to the previous paragraphs on encryption

Sources: Facebook Note

Issues for LEA

Data that is not accessible and stored for short periods of time make it more difficult to fight crime

- encryption makes it difficult to access data that is needed to fight crime
- there is a lot of crime on the internet
- connect it specifically to Facebook and their proposals
- specifically cse from Open letter and NYT
- Facebook acknowledges that it will be hard to do with e2ee

Sources: Facebook Note, Open Letter, OECD, NYT cse piece

Proposing backdoors in the Open letter

Facebook should provide access to users' data in a readable and usable format – backdoors into their encryption

- see above in general discussion on backdoors what kind of mess this would be
- it would invalidate the whole idea that Zuckerberg was proposing

- OECD guidelines and the problems the reference in connection to this proposal

Source: OECD guidelines, Open Letter, Keys Under Doormats

Contrasting the EU approach with the Open Letter approach

Reasons for the debate

While the open letter takes cse as the main reason, the EU uses terrorism as the main reason

- terror attacks in Europe and the following debate – how it started
- Open Letter is more of a continuation of the Crypto Wars than a new thing
- does that ultimately make a difference?
- security alliance and CLOUD ACT on UK side as well

Source: Open Letter, Debate Summary, Keys Under Doormats

The European Approach

The EU holds encryption to be very important and does not endorse weakening or backdoors

- state where the EU says that encryption is important
- where do they say they will not try to weaken or backdoor it
- even Europol and ENISA agree that they will not push for that
- this precludes both common practices that were discussed previously

Sources: 11th progress report, Debate Summary, ENISA-Europol agreement

Possible alternatives

Because the ususal routes of regulating encryption are not open to the EU, they focus on different things – workarounds and other strengthening

- regardless of the previous statement, Europol and ntl LEA are not crazy about encryption so they have to do something
- example of circumvention would be FBI cracking San Bernadino shooter's phone without Apple's help
- debate summary on their plans, also 11th progress report
- strengthen Europol, national LEA, expert networks, cross-border cooperation
- they want to circumvent the problem if they can
- or Germany using viruses to get data before it can even be encrypted

Sources: 11th report, debate summary

Issues with that approach

The area is pretty uncharted and the countries might not work together effectively

- toolbox sharing might be difficult
- citizens state that they do want LEA to share info to solve crimes
- capabilities are very different
- there aren't really any laws about state hacking and that stuff
- it is a contradiction to support encryption and still try to beat it
- lack of transparency in the state capabilities, laws, EU procedures
- no EU mandate to really enforce any measures like that

Sources: debate summary, Keys under doormats?

Results so far

The debate is pretty young, so there are few actual results, but moslty strengthening Europol

- EP gets more money to improve their hacking capabilities
- national LEA are trained
- expert networks are created
- the conviction that a solution exists is there
- because terrorism was there at the start, the debate is less focused than it should be

---

Summary and outlook

It seems like there is no clear solution in sight

- interesting to see the EU taking such a different approach to the whole topic
- good to see fundamental rights being upheld by their approach
- as such they probably chose the most difficult path and the least trodden one

[1]: [https://www.google.com/publicdata/explore?ds=alp1i5f0htq8h_]