Introduction

- this presentation has a different structure than my paper – shows my ‘journey’
- wanted to work on encryption
- encountered the problems and the debate about encryption
- wanted to know what the answers were, if there were any
- found the example of Facebook Messenger which is current and important
- then I went on to see what the EU would say about this – prompted by a letter
- **became an analytical paper on what is encryption, debate in the EU, connection to Facebook’s proposal, possible solutions to the issue**
- **Who of you uses Facebook Messenger? WhatsApp? Instagram?**

Basics – wanted to do research on because of interest

- what is encryption?
- flowchart shows in the most general terms how it works
- caesar cipher is one of the simplest
- RSA is an asymmetric algorithm that is used today, here with 512 bit keys in base64 encoding
- these kinds of algorithms are basically unbreakable – it takes years, if not millennia to do so – and forward secrecy makes that useless

Problems – What are the problems I learned about

- like any tool, it can also be misused – can be used to hide crimes and even commit them
- Facebook Messenger is supposed to become more private and more secure
- this would make the detection of illegal content more difficult
- high numbers of *cse* and *terrorism* on FB and FBM – **big problem for LEA if all of that gets encrypted**
- because of how high social media use is and how many people use Facebook, this issue will have a high impact, regardless of the solution

Debate – the debate caused by problems I learned about

- how can LEA access information while not weakening the security of everyone?
- debate started in the ’90s – no solution was found back then
- *privacy vs security* is the fundamental question here
- Crypto Wars – old debate
  - weak encryption: bad because it is always weak
  - key-escrow: has many problems with management of keys and implementation
  - mostly driven by crime like cse, digital theft, money laundering etc
  - **FB proposal is not compatible with these measures**
- EU approach – new debate in the EU, still ongoing
  - supports encryption – strong and without key-escrow
  - seeks alternative measures: breaking encryption, cooperation between LEA, training programs
  - EU debate is driven by terrorism, not crime like cse
  - terrorism is also a priority for EU citizens
  - **this approach is actually compatible with FB’s proposal**

Solutions – proposed solutions to the problem I found

- EU approach differs from the failed earlier approach
- they support encryption
- access would be situational and there would be no weakness introduced into the system for LEA’s sake
- it will be difficult to break encryption, cooperate effectively with other national LEA
- is it too hypocritical to break encryption and celebrate it at the same time?
- how well this will even work remains to be seen