Outline - Encryption Debate in the EU

- 10 to 12 pages
- Open Data
- Data Visualization
- **use oecd guidelines**
- fbi suggestions to interpol regarding the encouragement of backdoors

Introduction

- hook with facebook and messenger and the debate around the subject
- Give a definition of encryption
  - encryption is … according to this authority on the subject
  - What is the primary goal of encryption?
- Why is this topic relevant in general
  - the internet is built on encryption technology
  - without it we could not do the stuff that seems normal to us now
    - online banking
    - private messaging
    - storing our data in the cloud
    - shopping online
  - everyone could read what you are sending and receiving
  - people would not trust the services if their data could be accessed by anyone
- **Relevancy in the EU could be established using the Eurobarometer**
- What is the debate about
  - all the good sides also have bad sides
  - there is a lot of crime on the internet
    - theft
    - child pornography
    - terrorism
  - some of these criminals benefit from encryption - makes them hard to catch
    - child pornography
    - terrorists
  - law enforcement agencies are obviously not happy with that
    - they want access to that data to fight crimes
  - data protection advocates and scientists are not happy with law enforcements solution as it poses a threat to the security of all users, not just the criminals that it supposedly targets
- Why the EU
  - in the EU we have the nice dichotomy between them heralding it as a savior of freedom of speech and demonizing it at the same time
  - Europol on the other hand is not liking it, as leas tend to do
  - so what are they doing now?
  - now with

Explain encryption

- primary goal
- how does is work in general terms
- how secure is it?
- backdoors
- end-to-end encryption and how it works with respect to facebook messenger
- strong vs weak encryption
- what is it most important for:
- some examples of common forms of encryption
  - TLS
  - https

  - ...
- the concept of “exceptional access”
- mention the effects of quantum computers on the debate if they become even better

Brief History of the Crypto-Wars that came before

- what was the issue back then?
- what were the arguments
- how was the problem resolved?
- how does this affect the current debate?
- security vs privacy is the age-old question regarding this issue and it is a philosophical one that has no easy answer

The problem in detail

- facebook, messenger, end-to-end and the cloud-act – letter to them by governments
- fbi vs apple on breaking the encryption of the iphone of one of the san bernadino shooters, apple refused, they used an isreali company to still break the phone and get the data from it
- **messenger already has e2e encryption, but not for groups**
- we’d like LEAs to be able to do their jobs, but putting everyone at risk is not a great look
- **use Eurobarometer to drive home the point of how normal europeans see this problem**
- law enforcement going dark
- information requests to google and co
- there are two main ideas of how they could still do their jobs
- separate master keys: agencies have master keys to the algorithm that allows them to read the encrypted data
- encryption is purposefully designed to be weak so it can be broken if necessary
- Europol Enisa agreement on no backdoors - what are they going to do instead?
- **Facebook and their messenger app as the main part of the whole paper?**
- criminals would just switch to secure services or build their own ones as it is not that hard to do if you are determined
- contradicting positions in the EU regarding this topic

How does the EU approach this problem?

- Europols approach
- ENISA
- Cloud act
- trying to either access data before it is encrypted - problems
- gearing up their cyber strength to be able to decrypt stuff regardless
- the contradicting positions the EU takes on the issue/ it is not one body but a behemoth of many smaller elements
- how could one form a coherent EU policy from this mess?
- UK is as of now still part of the EU, so what they do affects the EU as a whole
- EU members have very different approaches when it comes to dealing with encryption – common framework is needed
- e.g. Germany using viruses to get to data before it can be encrypted while other countries do other stuff – what issues does this have?
- there is a push for increased sharing of information between EU member states on this issue

What could be the solutions to this problem with respect to the EU and Facebook?

- I don’t know yet
- Medium article on that proposed solution?