Encryption Debate in the EU

Introduction

- encryption is an essential component of Europe's open markets and societies
- it is flourishing, but terror attacks caused the EU to start debating encryption
- europol and ntl lea called for a counter, as encryption was seen as a great threat
- this caused members to demand a policy solution and started a big debate
- current debate reminds of the zero-sum debates of the Crypto Wars
- how could fundamental rights of citizens and cross-border networks work under EA and how can the EU promote strong encryption without creating a safe haven for criminals?
- there is no solution in sight and the current Commission will probably not legislate anything before its term ends
- what they are doing is increasing Europol funding and training LEAs and cosulting with people – gaining a deeper understanding of the issue

Background

- terrorism is one of the main causes of this debate in the EU
- attacks in 2014, 15, 16 intensified fears
- IOCTA 2016 pointed to encryption as a major threat to terrorism investigations -> some member states demanded a policy solution
- other tensions are: Commission recognizing encryption as essential to protect personal data and the EU fundamental rights agency has heralded it too
- LEAs on the other hand warn about cse, corruption, cyber crime in general
- member states have different capabilities and rules when it comes to accessing data, slow cooperation

Key Actors

- for EU regulation: Germany, France, UK: took positions, called for legislation, are passing ntl legislation – they elevated the discussion to the EU level
- against EU regs: academics, technologists, civil society organizations like Access Now and European Digital Rights – demanded public discussions and information, urged the council to reject policies undermining strong encryption, made debates available to the public
- business interest groups called for encryption to be encouraged as a form to protect important business information
- people want independent oversight and enforcement
- VP for Digital Single Market opposes laws that force companies to use weak encryption or create backdoors
- Europol and Eurojust are observing the process; Europol and ENISA worked out a deal that opposes forcing companies to provide backdoors as those are not a secure fix and increase the attack surface, having wider implications for society
- still, in 2016 IOCTA Europol complained about maybe going dark, as encryption is the biggest problem they face when dealing with encryption, days before signing the ENISA agreement
- it's in doubt how effective any of this could be, the EU has no mandate on enforcing stuff related to criminal investigations, member states need to do it – some member states do not have the money or tech to enforce such legislation
- member states also have different experiences with the problem – different capacities for dealing with the problem; legal cooperation is not up to par
- new EU regs would then rely on these insufficient systems of enforcement
- Europol is encouraging member states to develop their own arsenal of decryption tools to break encryption without backdoors; urged stronger LEA cooperation for the lawful breaking of encryption
- "a solution that strikes a sensible and workable balance between individual rights and protection of EU citizen' security interests can be found."

Main Issues

September 2016 EU Council Questionnaire

- fears about going dark were escalating; EU interior ministers met in July to discuss the issue
- France and Germany signed a joint letter to the commission calling for a European solution to encryption
- questionnaire to EU interior ministers to find LEA issues
- problems of member states with encryption:
  - lack of technical expertise, processing power, no frameworks for cross-border cooperation
  - most common problems were full disk encryption and e2e messaging services; **all the popular and good services are also used by criminals**
  - 5 countries want easier access to encrypted data through EU legislation
  - access to cloud data stored outside of the 28 was asked for
  - most want more money for their police force as they lack the tech
  - most focused on data as evidence, not for surveillance
- December 2016 meeting on encryption issues around terrorism, new mandate for the commission to find technical, legal and political issues surrounding encryption in order to be able to find solutions that balance individual rights and LEA's ability to perform their duty
- new mandate made them explore aspects and implications of encryption through consultations, EU agencies, member state's LEAs, industry, academia, civil society

October 2017 EU Commission Position

- first announcement on position; support measures:
  - support Europol and its decryption abilities
  - expert network to support ntl law enforcement
  - toolbox for alternative investigation techniques that can get to encrypted information
  - better cooperation between member states and all involved parties
  - 500.000 euro for ntl training stuff
  - continued assessment of the role of encryption is criminal investigations
- this was embedded in the anti-terrorism package, framed encryption as a setback to LEA
- it **also** stated that encryption is vital personal data and cyber security
- encryption will not be inhibited or weakened with these rules
- this leaves a spot for future backdoors and the workarounds for encryption are not really addressed

Technical Measures

- EU does not want backdoors, but a more hands-on approach of just breaking the encryption themselves
- it is not declared how exactly this will work, but not weakening encryption while at the same time trying to break it is strange
- there is no real legal framework for state hacking and encryption workarounds, so all the work is being done in a legal vacuum
- **First Report of the Observatory Function on Encryption**
- it's difficult because of all the difference between agencies and states in the EU – still strong foreign encryption will be hard to break and without some encouragement member states will hardly share their tool boxes with other states

Related Issues

- 2014 EUP passed resolution as response to the Snowden papers to develop EU focused stuff to become more independent of the US tech sector
- e-evidence as cross border sharing of information
- on the other hand encryption is a strong component of EU policy regarding digital privacy
- **GDPR on encryption**

- how wiretaps of encrypted communications will be handled is still a question – how exports of encryption technology should be regulated is also to be seen

Outlook

- Commission will continues their consultations on this issue
- the new commission will then hopefully go public with their stuff
- **what have they done up until now?**
- the conflation of counterterrorism and encryption has made the debate unfocused, thus muddling the waters of the debate – it neglects the huge potential and use cases that encryption has
- there are calls for greater transparency about government hacking capabilities and what technical measures they actually have
- also how fundamental rights will be protected
- no mandate on legislating encryption