Decoding OECD Guidelines for Cryptography Policy

- sets out 8 principles for members to establish their cryptography policy

Background

- p. 729 “Cryptography is a means of putting data in code. It allows people to transform a message or data into a form that can’t be understood (decrypted) without knowledge of some secret information”
- p. 730 summary of how encryption works and does its thing
- secret key and public key cryptography
- there is also message authentication

Gov regulation

- encryption provides ways to use modern communications with complete security
- governments are not happy about this as criminals can also use that
- otherwise it allows people to share important information with people all over the world
- governments thus want to find a compromise
- one general solution is key-escrow where a person leaves an encryption key with a trusted third party; they key can be returned when the person needs it or dies or something; the gov could thus get lawful access to encrypted info
- contra to this is that criminals and terrorists would not participate in this and thus it would only hurt the normal people that cooperate
- some countries restrict the domestic use of encryption, others have export controls and try to influence international markets through that

OECD

- it makes suggestions about a host of topics but has no actual legal powers

Background of the Cryptography Guidelines

- unusual: very fast, only one year
- initiated by the US, other countries did feel the same problems
- generally those consultations are private, but this one was super public
- it showed the public’s interest

General Recommendation

1. document lists some other documents that relate to the issue at hand
2. setting out the concerns: growth of global information systems, commercial potential of those, importance of security for the realization of that potential
3. recognizing: what cryptography contributes to society
    - confidentiality: can protect and not using it can compromise data; cryptography can not be 100% secure, also needs good practices
    - authentication
    - anonymity
    - integrity of data
    - can also be used for nefarious purposes -> need balanced policies
    - as the internet is global, national rules do not make sense

Recommendations

- they want members to implement and adapt the recommendations
- also governments should make their decisions public
- members should avoid policies that create obstacles
- making the recommendations public is also a break while before it was often kinda obscure

Guidelines

- here are 8 principles:
- they want to promote the use of cryptography to secure networks
- to promote the use of encryption without jeopardizing safety and security
- we need compatible cryptographic systems that make interoperability easier
- all have interoperability in common
- aimed at governments, but not their classified or secret data
- the phrasing here is pretty open and includes most of cryptography
- the guidelines by themselves are contradictory but they should be considered as interdependent
- there should be a balance between them, but it does not give guidance on that
- each government can use the guidelines with the amount of importance that they attach to them; but all of them (except lawful access) must be given some weight

Principles

1. **trust in cryptography**: otherwise the systems using it will not be trusted; there is a lot of competition and rumors about products etc; govs should foster instead of undermine faith in encryption; one thing might be to list all the countries that could lawfully demand the keys
2. **choice of cryptographic methods**: choice is necessary for trust; encryption might be mandated when data is handled; this choice is of course limited by local laws, but that should be as minimal as possible, and no new laws should be created; there is nothing said about who can choose the method of cryptography in what circumstances, so can employees choose which C to use on their employers network?
3. **market-driven development**: market-driven makes some sense; it's open enough that governments can impose control over the market and demand that the market fulfills their demands; also argues for less overall government interference
4. **standards for cryptographic methods**: govs, experts and agencies should create standards, protocols and criteria for cryptography responding to the needs of the market; ntl standards should be compatible with intntl ones, to guarantee interoperability; tests, products, services should all be interoperable, consistent and accepted; interoperability: different methods can work together; portability: adaptation to any system; mobility: usage is possible in multiple countries/infrastryctures
5. **protection of privacy and personal data**: natl policies and implementations should reflect this; problem is that US and EU understand this thing very differently: protection agains gov vs. protection against companies as well; only private communications are treated as protected, not corporate ones
6. **lawful access**: lawful access may be allowed, but all the other principles must be protected to the greatest extend possible; stands out as it does make a recommendation: it just says that govs might, not that they should; also the whole thing puts this points below all the other 7 in this document
   - lawful access: access to data, keys or plaintext by authorized entities;
   - in accordance with law: there has to be a legal process involved when gaining access; access should be logged to insure legality; rules regarding access should be clearly stated
   - access to signature keys: these keys should not be made available to anyone without the consent of the owner of the key
   - providing vs verifying identity: public key verifies identity while the private one provides it; govs should not access the private one
7. **liability**: who is liable in case something goes wrong? comps wants to be secure in data so they move to encryption; certain encryption might be used as it is endorsed by the gov, so flaws don't

reflect on the comps using it as much; holders of keys could be liable if they fail to give it out; gov might be liable if the key they lawfully get is misused

  - contract vs. legislation: liability should first be imposed by contract and then by law to ensure the largest possible market
  - market scenarios on liability: quick key access with little security might be cheap; slow key access with high security might be very expensive; works if the market can decide what to do
  - enforcing these rules: need very clear framework for the liability, even if most of it is left to the companies
  - 3rd party liability: if a third party gets injured through a contract they are not a party in, how will the damages be handled?
  - where is legislation needed: negligence with private signature keys needs to be prohibited; keyholders cannot be held liable for compliance with lawful access; lawful access parties should be held liable for misuse of the keys they hold

8. **cooperation**: obstacles should be avoided, cooperation should be the norm