Argument Map
Restricting encryption

What are the arguments for and against a Dutch law that compels OTT service providers to be able to decrypt communications for law enforcement?

Pro

Safety

The law helps ensure national security and prevent and solve (serious) crimes

- Law enforcement gains access to channels that contain ever more relevant information.
- In particular, the law helps combat child pornography, terrorism and organized crime.
- Detection becomes more effective because there is always reliable access to encrypted communications.
- The law discourages criminals to commit crimes because it increases their chance of getting caught.

The law makes ensuring safety and security cheaper and more efficient

- The law makes access to encrypted communications cheaper and quicker than current alternatives.
- The law also gives law enforcement with limited resources access to encrypted communications.
- Criminals will switch to a limited set of services, which will simplify the work of law enforcement
- The law makes it easier for OTT service providers to filter channels for content such as child pornography.

Fundamental rights

The law leads to equal protection of fundamental rights in the digital and physical domain

- The law is comparable to laws in the physical domain, like exceptions to the confidentiality of correspondence.
- Law enforcement will operate more transparently because they currently use mainly secret methods.
- Law enforcement needs the law to fight crime in a digital society.

The law leads to a more proportional use of law enforcement resources

- The law is legally and technically easier to limit than alternatives such as hacking powers.
- The law is less radical than proposed alternatives, such as a ban on online anonymity.
- The law offers an alternative to current methods that sometimes breach many people's privacy.
- The law reduces the need for law enforcement to deploy drastic means, like infiltration.
- The law makes citizens and businesses feel better protected against online crime.

Economics

The law helps create a level playing field and fosters innovation

- OTT service providers will be under an obligation that already applies to other communications service providers.
- Companies will try to develop new encrypted services that fall outside the law.

Politics

The law is politically desirable

- The government can show that it is taking tough measures to tackle serious crime.
- The government can show that it can impose regulations on large businesses, including tech companies.
- The law shows that the Netherlands takes its international obligation towards law enforcement seriously.

Con

Safety

The law is not necessary for investigations and national security

- Law enforcement already has enough methods at their disposal to crack encryption, like hacking powers.
- Law enforcement has enough powers but lacks the resources to exercise them.

The law will do little to make the Netherlands safer

- Criminals will switch to using encrypted services that are not covered by the law, e.g. Encrochat.
- The chance exists that (some) OTT service providers will refuse to comply with the law.
- If OTT service providers leave the Netherlands, their services will still be accessible here, albeit illegally.
- Users will be more careless with information on OTT channels because they feel more secure.
- Law enforcement doesn't have enough capacity to make use of all the information that the law will provide.

The law presents a security risk to citizens, vital industries and the government

- The law will make OTT services more vulnerable to abuse by criminals and states worldwide.
- States will be more easily able to hack into OTT communications by the government and vital industries.
- Vulnerabilities in OTT services will make other systems that build on them unsafe, like online banking.

Fundamental rights

The law constitutes a disproportionate breach of privacy and freedom of speech

- The law makes end-to-end encryption impossible, currently the best communications security available.
- Law enforcement will gain access to the communications of many non-suspects like through group chats.
- The law undermines societal processes that require confidentiality, such as in journalism.
- People will censor themselves more if they know the government has acces to their communications.
- Societal pressure to monitor more online content will increase if it is technically possible.
- The government has not sufficiently explored the alternatives and their impact on fundamental rights.

The law makes it difficult to safeguard fundamental rights

- Countries without a robust rule of law will also compel OTT service providers to decrypt communications.
- Countries will attempt to access people's communications in the Netherlands, legitimately or otherwise.
- Deciding which countries may use the law and under what circumstances is legally complex.
- The law is a prelude to further investigation methods, such as tapping into other online services.
- Users of encrypted services that fall outside the law may be wrongly deemed as suspects.

Economics

The law undermines economic development and innovation

- The law stifles economic activity for which secure communications and trust in them are essential.
- The law will stifle economic activity if OTT service providers pull out of the Netherlands because of it.
- The law may reduce the use of OTT services because people know the government has acces tot them.

The law puts OTT service providers at a disadvantage

- The law forces OTT service providers to make their services less secure and therefore less attractive.
- OTT service providers have to adapt their systems, driving up costs and putting pressure on quality.
- Regimes without a robust rule of law will pressure OTT service providers to give them access as well.

Politics

The law forms a political risk

- The government shows that it places little importance on fundamental rights and secure communications.
- The government will be signalling that it does not place enough priority on the security of digital infrastructure.

The law is indicative of inconsistent government policy

- In 2016 the Cabinet affirmed that it placed great importance on digital security and encryption.
- Other laws, such as the privacy regulation require businesses to maximize information security.

About this map

This map sets out the arguments pro and con a law that would compel over-the-top services (OTT services) – upon lawful request – to give law enforcement access to communications in a readable form, for example by decrypting them. The arguments have been formulated form the perspective of the Netherlands, and do not necessarily apply to other countries. The premise of this map is that the law does not dictate which mechanism OTT service providers must use to decrypt communications. The definitions of the terms used in this map are printed on the reverse side. They may sometimes differ slightly from the usual definitions.

The reason for producing this map is a bill announced by the Dutch Ministry of Justice and Security in March 2021 that is expected to be submitted in a new cabinet period. The bill comes in addition to existing digital and other investigative tools, such as hacking powers, which in certain cases entitles law enforcement to engage in the remote penetration of automated information systems, such as smartphones and computers.

This Argument Map was commissioned by the Amsterdam Internet Exchange (AMS-IX) and the Platform for the Information Society (ECP) and made by De Argumentenfabriek. The arguments presented on this map were gathered in three thinking sessions with a broad group of experts from companies, governments, knowledge institutes and non-governmental organizations (see the reverse of this map). We would like to thank everyone for their efforts.

commisioned by: amsix ECP Platform voor de InformatieSamenleving

made by: De ArgumentenFabriek De Argumentenkaart

Argument Map
Restricting encryption

Terms and definitions
Over-the-top (OTT) services/service providers: generally available communications services that work services such as WhatsApp, Signal, Telegram and iMessage that operate using the public internet, often with their own end-to-end encrypted connections.
Encryption: the securing of digital communications using a mathematical technique designed so that they can only be read by the sender and the intended recipient(s). Encryption that is not end-to-end encrypted creates the possibility that the service provider can also read the communications.
End-to-end encryption: encryption designed in such a way that the communications can only be read by the sender and the intended recipient(s).
Decryption: making encrypted information readable again.
Law enforcement: law enforcement and intelligence services. Law enforcement are government agencies charged with detecting criminals and criminal offences, such as the police. Intelligence services are the Dutch General Intelligence and Security Service (AIVD) and the Dutch Military Intelligence and Security Service (MIVD).
Law: a law that would compel over-the-top services (OTT services) – upon lawful request – to give law enforcement and intelligence services access to communications in a readable form, for example by decrypting them.

Organizations involved
This map was commisioned with the help of experts from the following organizations:

Radiocommunications Agency Netherlands, Apple, Bits of Freedom, Dutch Cyber Security Council (CSR), European Parliament, Online Child Abuse Assessment Bureau (EOKM), Facebook, Fox-IT, IBM, KPN Royal Dutch Telecom, Microsoft, Dutch Ministry of Foreign Affairs, Dutch Ministry of the Interior and Kingdom Relations, Dutch Ministry of Defence, Dutch Ministry of Economic Affairs and Climate Policy, Dutch Ministry of Justice and Security, National Cyber Security Centre, Netherlands Forensic Institute, Northwave, Dutch Association of Journalists (NVJ), Netherlands Public Prosecution Service, Open Future Foundation, Amsterdam Police Force, High-Tech Crime Unit of the Dutch Police Services Agency, Radboud University, Safetynet, TU Delft and the University of Amsterdam.

Each organization regards the arguments on the map from its own perspective, which means none of them needs to agree with all of the arguments and will weigh them differently.

commisioned by: amsix ECP Platform voor de InformatieSamenleving