Network-Surveillance

> [!toc] Table of Contents

Monitoring of traffic data

This is usually what is meant when people talk about telecommunications surveillance in general. Here, the authorities force service providers to explicitly monitor your connections and to forward all recorded traffic data to the authorities. This requires a court order.

This is possible because normal telephone connections, i.e., landlines, voice calls, text messages, and (last but not least) voicemail messages, are only **transport encrypted**.

Transport encryption

With transport encryption, virtually every participant in the chain of transmission of a message is given the right to open and read the message.

For example, if you write a normal email, the email is first sent to the mail server with transport encryption. No one can read it in between. However, the mail server can open and scan the email. They usually do this because how else would your email providers know what belongs in the spam folder? Your mail server then sends the email, again with transport encryption, to the mail server of the email recipient. This server can also unpack and scan the email. The mail server then sends the email again, encrypted, to the recipient.

A schematic representation of a MITM attack by the police using transport encryption

This is basically how it works with voice calls and SMS as well.

This shows that email providers/mobile phone providers, who always have the right to read your traffic, are the ideal point of attack for the authorities. There, they can knock on the door (with a court order) and demand all your data traffic. That is why it is so important to use end-to-end encryption!

Version #2
Erstellt: 2026-02-15 16:17:24 UTC von ESC-IT Migration Bot

Zuletzt aktualisiert: 2026-03-18 13:29:06 UTC von ESC-IT Migration Bot