LAW ENFORCEMENT DISCLOSURE REPORT UPDATE

For our full year reporting, see latest report (January – December 2020) here.

Authority requests* January–June 2021

	Lawful interception	Historical data	Subscription data	Challenged/rejected requests
Denmark	2 330	874	3 841	0
Estonia	No stat's available (1)	5 599	431 144 (2)	12
Finland	3 461	2 379	5 103	37 (3)
Lithuania	No permission to publish (4)	50 419	44 943	24
Norway	507	3 838	5 056	13
Sweden	2 041	3 266	1 449	106

* As explained below, direct access is not included in the statistics.

1) Due to the technology used, Telia Estonia has no visibility on the data regarding Lawful interception.
2) Includes all requests for Subscription data. For other countries the corresponding figure covers only requests that are handled by authorized personnel, as well as automated requests that refer to criminal cases.
3) It is noted that Challenged/rejected cases are in most cases related to erroneous target information from the Police.
4) Telia Company and Telia Lietuva have not been granted permission to compile and publish our own statistics regarding how many lawful intercept requests we have received in Lithuania. See page 10 in the 2020 annual Law Enforcement Disclosure Report, here.

Purpose of the Report

Telia Company is committed to respect freedom of expression and the privacy of users. This report reflects our aim to provide insights into the extent of authorities' collection of customer data for law enforcement purposes. Operators must adhere to law enforcement requirements which may impact an individual's freedom of expression and privacy. What Telia Company can do is to challenge such requests if they have no or unclear legal grounds, advocate for necessity and proportionality and inform customers and stakeholders of the extent of such surveillance, including the legal context.

Through Law Enforcement Disclosure Reporting we aim to provide transparency around surveillance, build user trust and gain the confidence of stakeholders by reflecting how we manage human rights risks related to freedom of expression and privacy. Furthermore, we aim to contribute to meaningful oversight and discussions regarding the proper limits of government surveillance powers.

Challenges and limitations

Several factors make it difficult to compare information over time as well as between markets, see the Q&A about Telia Company's Law Enforcement Disclosure Reporting and our latest full year report published in March 2021, both available here, for elaboration on such challenges.

Most notably, governments have direct access, i.e. real-time network access without requests, e.g. signals intelligence (intelligence gathering through analysis and processing of communication signals) and technical systems for more extensive monitoring of telecommunications. With regards to such direct access, Telia Company has no insight into the extent of surveillance and cannot provide statistics. What we can do is to publish links to relevant legislation providing for the authorization of direct access to governments in our respective markets (see further pages 7-8 in the 2020 report).

Definitions

By '*Lawful interception'* we mean secret real-time wire-tapping and monitoring by the police and secret police, e.g. real-time access to the content of communications or traffic data ("listening in", wire-tapping, checking who is calling who, when and for how long or access to location information or internet traffic). In some countries, lawful interception requests may include requests for historical data. In order to avoid duplicate reporting, these are not reported separately below in 'Historical data'.

By *'Historical data'* we mean historical traffic data, location data on mobile devices and cell-tower dumps. Traffic data relates to the use of telecommunications services including call data records, SMS records and internet records. These records include information such as the number of a called

party and the date, time and duration of a call. Internet session information includes the date, time and duration of Internet sessions as well as email logs. This figure also includes manual emergency positioning requests by the emergency centers and police. (Emergency positioning is normally automatically initiated after a call to the local emergency number, e.g. 112.)

By *'Subscription data'* we mean secret numbers and information about supplementary services. Subscription data refers to details that appear on a bill, such as the customer's name, address and service number. It can also include other information we may hold, such as a customer's date of birth and previous address as well as the identity of the communication equipment (including IMSI and IMEI). This figure consists of requests that are either handled by authorized personnel or by an automated interface with reference to a criminal case identification number.

'Challenged/rejected requests' contain information on how many requests we have challenged, for example by asking for clarification, the correction of formalities or by rejecting the request. All requests from authorities must be legally correct. Telia Company will challenge or reject any request that does not conform to the established form and process, for example, when a form has not been signed or not been sent by an appropriate sender.