LAW ENFORCEMENT DISCLOSURE REPORT UPDATE

Authority requests* January–June 2019

Country	Lawful interception	Historical data	Subscription data	Challenged/rejected requests
Denmark	4 734	1 304	6 818	0
Estonia	No stat's available *1	7 776	403 602 *2	14 *3
Finland	2 590	1 328	6 323	28 *4
Moldova	No statistics available	3 527	1 202	59
Norway	572	2 444	5 066	20
Sweden	1 920	2 629	836	176

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

* 1 Due to technology change, Telia Estonia has no visibility to data regarding Lawful inception.
* 2 Includes all requests for Subscription data. For other countries the corresponding figure covers only requests that are handled by authorized personnel, and automated requests that refer to criminal cases.
* 3 The reporting now changed in the way that requests regarding subscribers belonging to other operators are no longer included in this figure.
* 4 Telia Company has informed the Finnish police about the significant increase in this number, largely depending on Telia requesting forms to be filled in correctly. It is also noted that Challenged/rejected cases are in most cases related to erroneous target information from the Police.

Telia Company and Telia Lietuva have not been granted permission to publish statistics regarding how many requests we have received in Lithuania. See the full Law Enforcement Disclosure Report published March 2019, page 22, for further information.

About the Law Enforcement Disclosure Report

Telia Company's Law Enforcement Disclosure Reporting (LEDR) aims to provide insights into the extent of authorities' collection of customer data for law enforcement in six of Telia Company's markets. The latest full report can be found here. Our aim is to contribute to a meaningful overview and discussion of the proper limits of government surveillance powers. Maintaining customer privacy is of the utmost importance to Telia Company. At the same time, Telia Company and its local subsidiaries – like all telecommunications companies – are obliged by legislative, administrative, license or law enforcement requirements to respond to requests and demands from authorities to disclose customer information. Such obligations are specified by law and based on specific reasons, including enforcing criminal law and safeguarding national security.

We are to disclose information to surveillance authorities only to the extent required by law. This commitment is incorporated in our policies and procedures and is a non-negotiable part of the way we operate. It should be noted in this context however that governments also have direct access, i.e. real-time network access without requests in the form of signals intelligence and technical systems for more extensive monitoring of telecommunications without having to send requests to operators. Regarding such direct access, operators have no insight into the extent of surveillance and cannot provide statistics. This is why we publish, each March, a chart in our full LEDR with links to legislation providing the authorities with such real-time direct access.

We provide statistics covering requests from the police and other authorities in Denmark, Estonia, Finland, Moldova, Norway and Sweden. The table above shows the number of authority requests based on a court order or other legal demands by the police or other authority between January and June 2019.

Challenges and limitations

Several factors make it difficult to compare statistics between countries. Telia Company has different market shares in different countries, which is probably reflected in the figures. Furthermore, Telia Company does not have knowledge of the working methods of the authorities or priorities in different countries, but the methods are likely to differ. Also, there are different working methods within different countries in Telia Company. This leads to issues related to completeness and accuracy of reported data.

Also note that the figures show the number of requests from authorities, not the number of individuals that have been targeted. Not even we as an operator and provider of the information have this knowledge. Most likely, in the category of lawful interception, the number of requests is larger than the number of individuals that have been targeted.

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 dial to the local emergency number, i.e. 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' contains information on how many requests we have challenged, for example by asking for clarification, the correction of formalities or 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 has not been sent by an appropriate sender.