TELIA COMPANY LAW ENFORCEMENT DISCLOSURE REPORT JULY TO DECEMBER 2017

Executive summary

This is Telia Company's eighth six-monthly Law Enforcement Disclosure Report. The report aims to offer detailed insights into the context and extent of surveillance and collection of, customer data in most of Telia Company's main markets. It includes statistics on conventional requests in eight of our markets as well as information, as regards all of our markets, on legislation regarding 'direct access' and unconventional requests ('major events').

A summarized version of this report is published in the Telia Company 2018 Annual and Sustainability Report available at annualreports.teliacompany.com. This full report includes more context, including such as information on main goals, definitions, challenges as well as omissions related to our reporting and a list of laws providing governments with direct access, and – added in this report - national laws on mandatory data retention for law enforcement purposes.

CONTENTS

Letter from the general counsel **3**
About this report **4**
What we report 4
Main goals 4
Included in this report 5
Challenges and omissions 5
Main challenges 5
Omissions 6
Law enforcement disclosure report summary (assured) **7**
Authority requests 2017 7
Statistics **9**
Authority requests* July – December 2017 9
Authority requests* January – June 2017 9
Authority requests* July – December 2016 10
Authority requests* January – June 2016 10
Authority requests* July – December 2015 11
Authority requests* January – June 2015 11
Definitions **12**
Authority requests – categories in the above tables 12
Different types of requests from authorities 13
Unconventional requests and demands **14**
Telia Company's assessment tool 14
A. Unconventional requests and demands from 2013 to 2015 15
B. Unconventional requests and demands January to June 2016 15
C. Unconventional requests and demands July to December 2016 15
D. Unconventional requests and demands January to December 2017 15
Transparency as to specific unconventional requests **16**
Laws providing governments direct access **17**
Laws on mandatory data retention for law enforcement **21**
Government law enforcement disclosure reports **22**
Additional transparency **23**
Questions and Answers **24**

LETTER FROM THE GENERAL COUNSEL

Millions of customers trust Telia Company to provide telecommunications services and to protect their communications, data and personal information. We publish Law Enforcement Disclosure Reports to contribute to an open and transparent world where freedom of expression and privacy are at the forefront.

Maintaining customer privacy is of utmost importance at Telia Company: It is one of the pillars of our Code of Responsible Business Conduct. 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 regulations and are based on specific reasons, e.g. enforcing criminal law and safeguarding national security.

According to our policies and procedures, Telia Company discloses information to authorities only to the extent required by law. This is a non-negotiable part of the way we are to operate. While our process is intended to identify and mitigate potential violations to individuals' freedom of expression and surveillance privacy, the actual outcome heavily depends on local laws as well as the security and capability of local employees. It should specifically be noted that, within this context, governments also have direct access, i.e. signals intelligence (intelligence gathering through analysis and processing of communication signals) and real-time access without any need to send requests to the operators (technical systems for more extensive possibilities to monitor telecommunications). Regarding such direct access, Telia Company has no insight into the extent of surveillance (when, who and what) and cannot provide statistics. What we can do is to publish, as in this report, links to such relevant legislations in our respective markets. From this report onwards, we have also added links to laws on mandatory data retention for law enforcement purposes.

The issues are complex. Different stakeholders have different views, and there are societal needs both for surveillance, security and privacy. Nevertheless, fundamentally we respect and support individual's rights to freedom of expression and surveillance privacy, even as we accept that sometimes there need to be limitations on those rights, to the extent international human rights frameworks allow. Limitations must be necessary and proportionate and clearly delineated within a strong legal framework with the right checks and balances. When there is an opportunity, we argue for legislation which supports and promotes freedom of expression and surveillance privacy.

We encourage governments to be transparent about their use and scope of surveillance of communications. We welcome reports – such as the ones in Denmark, Finland, Georgia, Lithuania, Norway and Sweden – where each respective government regularly and publicly reports about the scope of their surveillance.

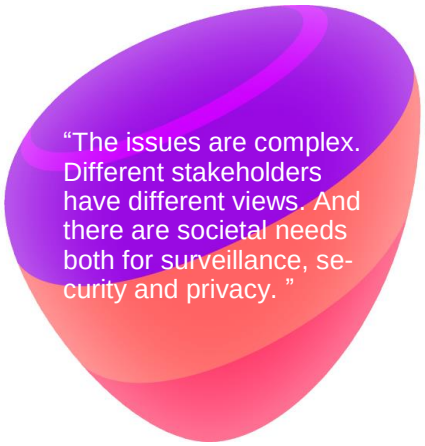
Although these publications might not always cover all kinds of requests and demands, we see publicly shared government reports as the preferred starting point for discussing best practice for meaningful transparency, based on the fact that a government can cover not only Telia Company's but all telecom operators in any respective country and also respond to any questions as to necessity and proportionality of surveillance.

To supplement government reporting, our aim is to contribute to a meaningful oversight and discussion of the proper limits of government surveillance powers. We plan to publish a full Law Enforcement Disclosure Report together with our Annual and Sustainability Report (every year in March) and an update of the statistics every October.

In this report, we continue publishing statistics covering requests from the police and other authorities in Denmark, Estonia, Finland, Georgia, Moldova, Norway and Sweden. We have also added figures provided by authorities in Lithuania. The tables included in this report show the number of authority requests in each country based on a court order or other legal demand by the police or other authority.

Stockholm March 20, 2018

Jonas Bengtsson
Senior Vice President and General Counsel
Telia Company



ABOUT THIS REPORT

What we report

This report covers:

- Statistics on the number of *conventional* ('day-to-day') law enforcement requests;
- Information about *unconventional* ('major') government requests; and
- Links to laws providing governments with direct access.

While retaining most of the explanatory text in this updated report, we have in this report;

- Updated statistics as to the eight markets we covered in our report October 2017; and also
- Added links to laws on mandatory data retention for law enforcement purposes.

We publish statistics covering requests from the police and other authorities in Denmark, Estonia, Finland, Georgia, Lithuania, Moldova, Norway and Sweden. We plan to publish a full Law Enforcement Disclosure Report together with our Annual and Sustainability Report (every year in March) and an update of the statistics every October.

According to our policies and procedures, Telia Company discloses information to authorities only to the extent required by law. This is a non-negotiable part of the way we are to operate. It should be noted that, within this context, governments also have direct access, i.e. signals intelligence and real-time access without having to send requests to the operators. Regarding such direct access, Telia Company has no insight into the extent of surveillance and cannot provide statistics. What we can do is to publish in this reporting a chart with links to legislation providing the authorities with such direct access.

Our next full Law Enforcement Disclosure report is planned to be published in March 2019.

Main goals

Our goal with this Law Enforcement Disclosure Reporting, our transparency reporting in the context of surveillance, is to build user trust and gain the confidence of investors that Telia Company manages its human rights risks related to freedom of expression and surveillance privacy. Our aim is also to contribute to meaningful oversight and discussions regarding the proper limits of government surveillance powers. By publishing law enforcement disclosure statistics, as well as thorough context, Telia Company wants to make it transparent to our customers and stakeholders to what extent authorities require access to data. We therefore;

- Report statistics also in markets where Governments themselves report;
- Seek to move beyond numbers, complementing quantitative transparency with context for these requests;
- Seek to disclose information that all stakeholders can understand, not just telecommunications regulators and policy specialists;
- Seek to provide evidence that we are embedding our freedom of expression and privacy commitments; and
- Advocate for legal and regulatory changes that protect the freedom of expression and privacy of our customers and users.

Our report aims to provide insights into the extent of authorities' collection of customer data for law enforcement purposes in, today, eight of our Telia Company markets. This is a part of Telia Company's commitment to respect freedom of expression and privacy. 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 inform its customers and stakeholders of the extent of use of such surveillance, including within which legal context.

Inevitably, Telia Company makes own judgments on these issues. We listen and participate in stakeholder dialogues. We welcome views on how we can improve.

We have also taken further steps to establish effective grievance mechanisms by including reporting on human rights violations into Telia Company's speak-up line, a whistle-blowing tool that enables employees and external parties to anonymously report violations at speakupline.ethicspoint.com. The effort to build a strong culture of transparency and non-retaliation continues. Relevant case reports are converted into ethical dilemmas that can be used to train employees and managers. Learnings from cases are used to provide targeted training for relevant management teams.

The tables show the number of authority requests in each country based on a court order or other legal demand by the police or other authority.

The categories of data reported are explained briefly below the charts and in more detail under the chapter 'Definitions'.

It should be noted that several factors make it difficult to compare the statistics between countries. Telia Company has different market shares in different countries, which is probably reflected in the figures. Furthermore, Telia Company is not privy to each authorities' working methods and priorities in different countries, and these methods are likely to differ as well. Also, within Telia Company, there are different working methods in different countries which causes issues related to completeness and comparability of reported data. See further the Questions and Answers (Q&A) section in this report titled "Why do the figures differ between countries". We

work to streamline these working methods and define best practice with the aim to further improve data quality.

It should, furthermore, be noted that the figures show the number of requests from authorities, not the number of individuals that have been targeted. Not even Telia Company as the operator and provider of the information has this knowledge. Within the category of lawful interception, the number of requests is most likely larger than the number of individuals that have been targeted.

As to requests for cell tower dumps (i.e. requests that oblige Telia Company to disclose data about the identity, activity and location of any device that connects to targeted cell towers over a set span of time) the number of affected individuals will naturally become significantly larger than the number of requests.

The statistics include figures from companies in our group, where Telia Company owns the networks and process for law enforcement disclosure. This means that our figures (except for the category 'Lawful interception') do not cover all requests directed to external service operations because these might be directly responsible for such as subscriber information requests.

Telia Company has committed itself to a Policy on Freedom of Expression and Surveillance Privacy. The Policy defines Telia Company's commitments in relation to *unconventional* requests or demands with potentially serious impacts on the freedom of expression and surveillance privacy. You can read about our commitments here Telia Company has committed itself to informing stakeholders of such events whenever and to the extent legally permissible and doable, taking the safety of our employees into account. Our aim is to publish information on each and every unconventional request or demand as soon as possible after having been notified. However, due to strict laws on confidentiality, or other circumstances such as the liberty and safety of personnel, it is often difficult or impossible to report on a specific event. This is why we publish, here below, short aggregated information on unconventional requests and demands, not mentioning the country in question.

Included in this report

Denmark: The statistics include figures regarding the police and the secret police.

Estonia: The statistics include figures regarding the police, secret police, Tax and Customs Board, Ministry of Justice and Estonian Foreign Intelligence Service.

Finland: The statistics include the police, secret police, and customs. In addition, figures regarding tax authorities are included, since in Finland the police investigate economic crimes in cooperation with the tax authorities.

Georgia: The statistics include figures regarding requests from courts. All surveillance authorities, such as the Prosecutor's Office of Georgia, the Ministry of Internal Affairs, and Tax Revenue Services, etc), send their requests via the courts.

Lithuania: The statistics include figures regarding the State Security Department of Lithuania, Lithuanian Criminal Police Bureau, Second Department of Operational Services under the Ministry of National Defense; provided by the authorities and reported by the Telia Company affiliate in Lithuania.

Moldova: The statistics include figures regarding the following authority organizations: Ministry of Internal Affairs, Ministry of Defense, National Anti-Corruption Centre, State Protection and Guard Service, Security and Intelligence Service, Customs Service, Penitentiary Department of the Ministry of Justice, Prosecutor's Office, Courts.

Norway: The statistics include figures regarding the Police, (politiet), Criminal Investigation Service (Politiets sikkerhetstjeneste), National Criminal Investigation Service (KRIPOS) and thePolice Security service (PST) and Rescue/Emergency Services (HRS).

Sweden: The statistics include figures regarding the police (which in turn include requests from the secret police), tax agency (Swedish: 'Skatteverket'), customs, the Enforcement Authority (Swedish: 'Kronofogdemyndigheten'), and the Economic Crime Authority (Swedish: 'Ekobrottsmyndigheten').

Challenges and omissions

Telia Company wants to be transparent on the main challenges regarding completeness in order to give the readers the possibility to understand the problems and make their own judgments.

Main challenges

- Governments have direct access, i.e. signals intelligence and real-time access without having to send requests to the operators. As 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 such legislation in our respective markets in the way we do in this report.
- Telia Company's internal systems for interaction with the authorities have been set up to handle each single interaction. This means that a request to extend or to discontinue on-going interception is counted as a request in the statistics. We continue to work towards better aligning our processes with the reporting needs in order to make our reporting more user friendly.
- With regard to the category of lawful interception, the number of requests is most likely larger than the number of individuals that have been targeted. Pertaining to requests for cell tower dumps (i.e. requests that oblige Telia Company to disclose data about the identity, activity and location of any device that connects to targeted cell towers over a set span of time),

however, the number of affected individuals will naturally become significantly larger than the number of requests. Depending on the scope of such a request, Telia Company is required to hand out varying amounts of customer data. This depends on the timeframe of the request as well as where the cells within the scope of the request are situated. In urban areas the amount of disclosed data is naturally higher.

Cell tower dump requests are part of the statistics provided in this report. In countries where these requests are part of the law enforcement measures, it is reported under the historical data category. We are not reporting these separately, but in the Nordics we usually receive roughly around 40-70 cell tower dump requests a month and per country. An answer to a cell tower dump request can include information from some few devices to even tens of thousands of devices.

We have sought to add additional of our markets to this Law Enforcement Disclosure statistics, e.g. statistics on the number of authority requests in additional operations in Eurasia. Telia Company in September 2015 announced to leave Eurasia over time. We will seek to promote the publication of similar reports by the local companies and their new owners.

Omissions

The following has not been included in this report:

Other than surveillance
Telia Company's statistics do not include requests from authorities that have no role in lawful interception or other services obligated for operators, such as requests from competition authorities and national regulatory authorities or requests based on the copyright IPR Enforcement Directive. Also, the report does not cover information on Telia Company's voluntary commitment to block child sexual abuse material based on a list from Interpol and/or local law enforcement.

Information on emergency positioning
Emergency positioning requests are outside the scope of surveillance. They are normally automatically initiated after a dial to the local emergency number (i.e. 112). We have, since July 2015, discontinued to include such automated positioning to this Report. We have however placed manual positioning requests, which are mostly done also for rescuing people, in the Historical data category.

Customer privacy
This report covers Telia Company's commitments as to freedom of expression and surveillance privacy and interaction with law enforcement authorities. Our commitments as to customer privacy, not covered in this report, are defined in our Privacy Policy, available here. Our work as to customer privacy is published in our Annual and Sustainability report.

Telia Carrier operations
Telia Company owns and operates one of the largest fiber-optic networks in the world, providing network infrastructure and services to more than 1,000 customers in 80 different countries worldwide. Telia International Carrier markets are not included in the law enforcement disclosure statistics in this report.

Requests or demands from private entities
Telia Company local companies are not to act upon requests or demands from private entities to remove, filter or restrict access to content. Telia Company, however, actively participates in combating spam, viruses and distributed denial of service (DDoS) attacks to protect our customers and networks.

LAW ENFORCEMENT DISCLOSURE REPORT SUMMARY (ASSURED)

The Annual and Sustainability Report 2017 has been subject to limited assurance. This summary is an extract from that report.

Law enforcement disclosure reporting
We believe that transparency on surveillance activities contributes to freedom of expression and surveillance privacy being more strongly enforced. This is why we publish law enforcement disclosure reports (LEDR) twice a year.

The most recent report, released alongside this Annual and Sustainability Report, includes statistics covering conventional ("day-to-day") requests from the police and other authorities in eight countries. The statistics show the number of authority requests based on a court order or other legal demand by the police or another authority. The statistics are subject to limited assurance by Deloitte.

Authority requests[1] 2017

Country	Lawful interception	Historical data*	Subscription data	Challenged/rejected requests
Denmark	8,130	2,057	12,225	0
Estonia	4,596[2]	1,327	386,606[3]	54,168[4]
Finland	3,640	2,474	7,436	20
Georgia	Direct access – no statistics	847	49	30
Lithuania	2,733[5]	No permission to publish	No permission to publish	No permission to publish
Moldova	Direct access – no statistics	9,464	5,002	175
Norway	1,569	6,315	9,201	68[6]
Sweden	3,822	3,255	1,521	200

1) As explained below, direct access is not included in the statistics.
2) In Estonia, a direct access system is used. Telia in Estonia has full visibility into the number of requests.
3) 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 a criminal case.
4) This figure includes all requests to which we were not able to answer, most often because the requested information was about a customer of another operator.
5) Telia in Lithuania have been granted permission to publish Lithuanian authority statistics for Lawful interception requests. Telia in Lithuania has added a few requests. According to the authority and Telia in Lithuania statistics, there were 2,733 requests during the year.
6) Invalid requests due to administrative form errors.

Telia Company has not been able to establish reporting of statistics on conventional requests in our operations in Azerbaijan, Kazakhstan and Uzbekistan.

Several factors make it difficult to compare the 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 authorities' working methods and priorities in different countries, but the methods are likely to differ. Also, within the group, there are different internal methods of collecting data in different countries causing issues related to completeness and accuracy of reported data. We aim to streamline these working methods and define best practice to further improve data quality. 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 the 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.

Pertaining to requests for cell tower dumps (i.e. requests that oblige the local operator to disclose data about the identity, activity and location of any device that connects to targeted cell towers over a set span of time) the number of affected individuals will naturally become larger than the number of requests. Depending on the scope of the request, Telia Company is required to hand out varying amounts of customer data. This depends on the timeframe of the request as well as where the cells within the scope of the request are situated. In urban areas, the amount of disclosed data is naturally higher.

Additionally, the LEDR includes links to national laws that provide governments with direct access to information about our customers and their communication without having to request information from Telia Company. Regarding governments' direct access, i.e. signals intelligence (intelligence gathering through analysis and processing of communication signals) and real-time access without requests (technical systems for more extensive monitoring of telecommunications), Telia Company has no insight into the extent of such surveillance (when, who and what) and cannot provide any statistics beyond those provided within this report.

Our reporting on country local laws on freedom of expression and surveillance privacy in telecommunications is performed through contributions to the ID/GNI database on country legal frameworks.

Unconventional requests
In addition to reporting statistics on conventional requests, we seek to publish information on unconventional requests or demands from governments ("major events"). During 2017, we closed nearly 30 such unconventional requests or demands from governments across our operations. To ensure consistency, group level experts facilitated local assessments and escalations. Points of challenge, where possible to establish and most often by being transparent, were defined jointly by local and group management. There are challenges related to transparency on unconventional requests. Local laws that sometimes lack full clarity determine what can be published. There may be confidentiality provisions and/or constraints based on our duty to protect the safety of our employees. Issues regarding direct access are closely related to national security and are therefore complex and challenging to communicate. Counting the number of unconventional requests is difficult and subjective as they range from a demand to block one or several websites or shutting down a network locally to requests regarding direct access.

STATISTICS

The information below is provided as it was reported in each respective earlier law enforcement disclosure report, adding in the first two charts below the figures for January to June and July to December 2017. Certain information, such as 'Emergency positioning' statistics and footnotes, remain as they were from earlier reports. Statistics covering periods further back in time can be found here .

It should be noted that the figures show the number of requests from authorities, not the number of individuals that have been targeted. It should also be noted that differences as to market share as well as the working methods of both authorities and within Telia Company make it difficult to compare statistics between countries.

Authority requests* July – December 2017

Country	Lawful interception	Historical data*	Subscription data	Challenged/rejected requests
Denmark	4,124	1,031	6,950	0
Estonia	2,503[1]	662	260,867[2]	53,518[3]
Finland	1,865	1,391	3,710	12
Georgia	Direct access – no statistics	396	15	29
Lithuania	1,366[4]	No permission to publish	No permission to publish	No permission to publish
Moldova	Direct access – no statistics	4,502	2,356	93
Norway	675	3,089	4,077	36[5]
Sweden	1,808	1,769	654	146

* As explained below, direct access is not included in the statistics.
*1 In Estonia, a direct access system is used. Telia in Estonia has full visibility into the number of requests.
*2 This figure includes all requests for Subscription data. For other countries, the corresponding figure only covers requests that are handled by authorized personnel, and automated requests that refer to a criminal case. This number has increased due to the implementation of a new system for automated queries. To get all information for an individual subscriber, a higher number of requests are needed.
*3 This figure includes all requests to which we were not able to answer, most often because the requested information was about a customer of another operator. This number has increased due to the implementation of a new system for automated queries. To get all information for an individual subscriber, a higher number of requests is needed.
*4 Telia in Lithuania have been granted permission to publish Lithuanian authority statistics for Lawful interception requests. Telia in Lithuania has added a few requests. According to the authority and Telia in Lithuania statistics, there were 2,733 requests during the year.
*5 Invalid requests due to administrative form errors.

Telia Company has not been able to establish reporting of statistics on conventional requests in our operations in Azerbaijan, Kazakhstan and Uzbekistan.

Authority requests* January – June 2017

Country	Lawful interception	Historical data*	Subscription data	Challenged/rejected requests
Denmark	4,006	1,026	5,275	0
Estonia	2,093[1]	665	125,739[2]	650[3]
Finland	1,775	1,083	3,726	8
Georgia	No statistics available	451	34	1
Moldova	No statistics available	4,962	2,646	82
Norway	894	3,226	5,124	32
Sweden	2,014	1,486	867	54

* As explained below, direct access is not included in the statistics.
*1 In Estonia, a direct access system is used. Telia in Estonia has full visibility into the number of requests.
*2 This figure includes all requests for Subscription data. For other countries, the corresponding figure only covers requests that are handled by authorized personnel, and automated requests that refer to a criminal case.

*3 This figure includes all requests to which we were not able to answer, most often because the requested information was about a customer not of our operations but of another operator.

Telia Company and Telia in Lithuania have not been granted permission to publish statistics regarding how many requests we have received in Lithuania. For further information, see the full Law Enforcement Disclosure Report.

Authority requests* July – December 2016

Country	Lawful interception	Historical data*	Subscription data	Challenged/rejected requests
Denmark	3,104	1,041	4,949	3
Estonia	1,965[1]	1,054	137,494[2]	655[3]
Finland	1,593	1,109	3,808	9
Georgia	No statistics available	230	147	277
Moldova	No statistics available	5,483	2,851	65
Norway	1,158	2,868	5,113	75
Sweden	1,643	1,278	737	68

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

*1 In Estonia, a direct access system is used. Telia in Estonia has full visibility into the number of requests.
*2 This figure includes all requests for Subscription data. For other countries, the corresponding figure only covers requests that are handled by authorized personnel, and automated requests that refer to a criminal case.
*3 This figure includes all requests to which we were not able to answer, most often because the requested information was about a customer not of our operations but of another operator.

Telia Company and Telia in Lithuania have not been granted permission to publish statistics regarding how many requests we have received in Lithuania. For further information, see the full Law Enforcement Disclosure Report.

Authority requests* January – June 2016

Country	Lawful interception	Historical data*	Subscription data	Challenged/rejected requests
Denmark	2,836	1,048	4,700	0
Estonia	1,438[1] and [4]	816	137,937[2]	928[3]
Finland	1,920	961	3,493	10
Georgia	No statistics available	328	129	126
Moldova	No statistics available	4,813	2,611	114
Norway	1,115	3,514	4,668	54
Spain	9,464	12,825	17,265	312
Sweden	1,782[5]	1,147	1,148	97

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

1 In Estonia, a direct access system is used. This figure has been provided by the Estonian authorities.
2 This figure, for Estonia, includes all requests for Subscription data. For other countries, the corresponding figure only covers requests that are handled by authorized personnel, and automated requests that refer to a criminal case.
3 This figure, for Estonia, includes all requests to which we were not able to answer, most often because the requested information was about a customer not of our operations but of another operator.
4 This figure has been corrected. Due to an editing mistake, the October 2016 report wrongly read 1483.
5 This figure has been corrected. Due to an editing mistake, the October 2016 report wrongly read 1728.

Telia Company and Telia in Lithuania have not been granted permission to publish statistics regarding how many requests we have received in Lithuania. See the full Law Enforcement Disclosure Report, page 20, for further information.

Authority requests* July – December 2015

Country	Lawful interception	Historical data*	Subscription data	Challenged/rejected requests
Denmark	3,000	661	4,687	27
Estonia	1,704[1]	990	133,687[2]	1,619[3]
Finland	2,207	1,129	4,312	14
Georgia	Not available[4]	90	560	241
Moldova	Not available[4]	5,261	2,816	101
Nepal	Not available[4]	18,220	20,519	0
Norway	988	3,002	4,762	83
Spain	10,183	16,177	20,112	339
Sweden	1,555	1,062	1,711	74

* Please note, as explained in the text, that direct access is not included in the statistics.

1 In Estonia, a direct access system is used. We keep a log of these requests.
2 This figure includes all requests for Subscription data. For other countries, the corresponding figure only covers requests that are handled by authorized personnel and automated requests that refer to a criminal case.
3 This figure includes all requests to which we were not able to answer, most often because the requested information was about a customer of another operator.
4 Statistics are not available

Authority requests* January – June 2015

Country	Lawful interception	Historical data*	Emergency positioning	Subscription data	Challenged/rejected requests
Denmark	2,825	707	145,305	4,985	11
Estonia	1,750[1]	1,236	900,390	154,736[2]	3,129[3]
Finland	2,187	949	422,260	3,555	12
Georgia	No statistics[5]	191	N/A[4]	743	635
Moldova	No statistics[5]	5,087	N/A[4]	2,714	134
Nepal	No statistics[5]	20,715	N/A[4]	16,503	0
Norway	1,396	2,232	74,865	4,411	44
Spain	10,230	18,902	601,358	23,877[6]	437
Sweden	1,395	788	782,291	2,306	162

* Please note, as explained in the text, that direct access is not included in the statistics.

1 In Estonia, a direct access system is used. This figure has been provided by the Estonian authorities.
2 This figure includes all requests for Subscription data. For other countries, the corresponding figure only covers requests that are handled by authorized personnel, and automated requests that refer to a criminal case.
3 This figure includes all requests to which we were not able to answer, most often because the requested information was about a customer not of our operations but of another operator.
4 No automated emergency positioning system in use.
5 Statistics are not available.
6 This figure has been corrected. Due to an editing mistake, the October 2015 report wrongly read '20,608'

DEFINITIONS

Authority requests – categories in the above tables

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 which 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.

Different types of requests from authorities

Like all telecommunications companies around the world, Telia Company is required by law to assist government authorities for defined purposes. Governments and authorities (e.g. the police, security authorities, and customs) conduct various types of surveillance of communications (e.g. calls, SMS, e-mail, surf) by imposing obligations on telecommunications companies in connection with criminal investigations and national security issues.

The government's surveillance of communications can be divided into four main categories

Surveillance **Category 1.** Requests from law enforcement authorities:

- Real-time access to the content of communications (e.g. listening in to voice calls) and access to historical content (e.g. checking what was written in an e-mail message)

- Real-time access to traffic data (e.g. checking who is calling who, when and for how long or internet traffic)

- Access to historical traffic data which the provider has stored or retained (e.g. checking who has called who, when and for how long)

- Access to subscription data which the provider has stored or retained (e.g. checking who is the subscriber of a certain telephone-number)

- Access to location information, i.e. access to information on the location of mobile terminals/phones (e.g. from which mobile cell a call is made)

Surveillance **Category 2.** Signals intelligence

Signals intelligence i.e. intelligence-gathering through analysis and processing of communication signals (example: the Swedish National Defence Radio Establishment; 'Försvarets Radioanstalt' in Swedish).

Surveillance **Category 3.** Direct access without requests

Real-time access without requests, i.e. technical systems for more extensive possibilities to monitor telecommunitions (ex: mass surveillance by national security authorities)

Surveillance **Category 4.** Shut-down, blocking, restriction of access, etc. ('unconventional requests and demands')

Examples: Shut-down of SMS-communication, blocking of the whole Internet or of certain web sites or requests and demands to install or up-grade systems for direct access.

This is how we publish information as to these four categories

Reporting on Category 1:

Telia Company Law Enforcement Disclosure Reporting on statistics. See this report, Chapter 'Statistics'.

Reporting on Categories 2 and 3:

Telia Company has no insight into the extent of surveillance and cannot provide any statistics. Telia Company has, however, added a list of national legislation within these two categories to this Report, see below.

Proposals for new laws or significant imposed operational changes in the area of these two categories may be defined as un-conventional requests ('major events') within Category 4.

Reporting on Category 4:

Telia Company reporting on unconventional requests and demands ('major events'). See this report, chapter 'Unconventional requests and demands'

UNCONVENTIONAL REQUESTS AND DEMANDS

Telia Company regards unconventional requests and demands from authorities which might potentially have serious impacts on the freedom of expression and surveillance privacy as 'major events'.

Governments' requests and demands often serve legitimate purposes such as the protection of certain human rights, but they may also be problematic in that they could conflict with other human rights. Our policy on freedom of expression and surveillance privacy defines Telia Company's commitments in relation to such unconventional requests or demands with potentially serious impacts on freedom of expression and surveillance privacy, such as direct network access, shutdown of networks and blocking of access to the Internet or specific websites. This is described in greater detail in the above chapter 'Definitions' under the head-line 'Different types of requests from authorities'. We also include and address initiatives for new law-making which might potentially have serious impacts on freedom of expression and surveillance privacy as 'major events', as we do with requests and demands to install or up-grade systems for direct access. Our commitments are available here.

Our aim is to publish information on each and every such unconventional request or demand as soon as possible after having been notified. However, due to strict laws on confidentiality, or other circumstances such as the liberty and safety of personnel, it is often difficult or impossible to report on a specific event. This is why we publish twice a year, here below, short aggregated information on unconventional requests and demands.

It must be noted that the below indication of the number of unconventional requests during a specific period, is quite arbitrary. If in one country a large number of websites have been blocked, and in another country only one, then each of these two count as one (1) major event in the figures below. A shut-down of the network or a service in *part* of a country is counted as a major event equally as a shut-down of the network or service in *all* of a country. A minor update of a system for government direct access to Telia Company's networks and services, e.g. SORM, is counted equally as a much more substantial upgrade of such a system. Etc.

Unconventional government requests are assessed by the local company and escalated within Telia Company for informed decision-making, including considerations from outside of the local context, on how to perform a point of challenge. This means adhering to the local law while at the same time seeking and performing measures to respect and support the rights of our users. We can request and remind that a decision be put in writing, postpone implementation to the greatest extent possible and/or seek to publicly share information about the request. While the process is intended to identify and mitigate potential violations to individuals' freedom of expression and privacy, the actual outcome heavily depends on local laws, the security and capability of local employees.

Telia Company's assessment tool

Within Telia Company, unconventional requests and demands are intended to be assessed and escalated in a way so that locally, regionally and group-wide, Telia Company can seek ways to respect freedom of expression and surveillance privacy. A tool for assessing and escalating has been elaborated and updated since adoption of the Telia Company policy, based on learnings from actual major events. The tool is available here .

A. Unconventional requests and demands from 2013 to 2015

Please see our earlier Law Enforcement Disclosure Reports, available here .

B. Unconventional requests and demands January to June 2016

Using the same set-up as introduced March 2016 in chapter C. above during the first half of 2016 we closed some 20 unconventional requests or demands from governments across our operations. Most of these were either about pro-longing or enhancing direct access based on local law, or new legislative proposals for surveillance. To support the decision making process and ensure a consistent view on freedom of expression throughout the group, we facilitated local company risk assessments and escalations. Points of challenge, where possible, were defined jointly by local, regional and group management.
In about half of these some 20 closed cases, Telia Company promoted freedom of expression, e.g. mainly by publishing information about them on teliacompany.com/news (see case studies in the Chapter ‘’Transparency as to specific unconventional requests’ here below), Were possible and relevant, we also pushed our views in specific and direct meetings with decision-makers. Additionally, in one case, the implementation was notably delayed.

As to direct access, e.g. SORM and similar systems, we are pursuing our point of view based on our Freedom of Expression Policy. The main difference between direct access and other systems is the legal framework through which law enforcement agencies can monitor citizens. Telia Company has, as has been reported in earlier versions of this report, challenges to push back and promote freedom of expression in the context of Government direct access. Several requests regarding SORM were closed at the beginning of 2016. Such requests are most often strictly confidential.

In one of our geographies, it is still difficult for the local company to receive the unconventional requests other than by e-mail despite the law requiring such requests to be in writing.

C. Unconventional requests and demands July to December 2016

Just as during the first half of 2016, during the second half of 2016 we closed some 20 unconventional requests or demands from governments across our operations. More than half of these requests were about blocking of lists of sites and/or of lists of open VPNs. Requests to block VPNs is a new type of request received. During this second half of 2016, we only succeeded in promoting freedom of expression in about one third of the events. More than half of the cases in which we could not promote freedom of expression were requests in a specific country. In one country, it is still difficult to receive, even in retrospect, specific requests other than by e-mail, despite the law requiring such requests to be in formal writing. There are challenges when seeking to be transparent. Local laws sometimes lack full clarity in determining what can be published. There may also be confidentiality provisions, and/or constraints based on our duty to protect the safety of our employees.

D. Unconventional requests and demands January to December 2017

During 2017 we closed some 30 unconventional requests or demands from governments across our operations. Roughly, one fourth was about blocking or restricting access to specific services, Internet websites or content. The remaining unconventional requests were more or less equally divided between; new surveillance legislation; data retention obligations; requests relating to existing legislation regarding unrestricted real-time network access; and ‘other’. Telia Company has been able to perform some kind of point of challenge in more than half of these requests and demands, either by being transparent (in some 50 percent of these cases), or by some other measure.

TRANSPARENCY AS TO SPECIFIC UNCONVENTIONAL REQUESTS

Telia Company aims to publish information on each and every unconventional request or demand ('major event') as soon as possible after having been notified. However, due to strict laws on confidentiality or other circumstances such as the liberty and safety of personnel, it is often difficult or impossible to report in detail, or even to be transparent at all, revealing the specific country. This is why we publish, above in this Law Enforcement Disclosure Report, aggregated information on unconventional requests and demands.

When it *is* possible to be transparent on some or all relevant information as to a specific unconventional request, Telia Company does so by publishing articles on www.teliacompany.com/news. Here examples of such articles during 2017;

Requests for user data in Denmark, Finland and Sweden
https://www.teliacompany.com/en/news/news-articles/2017/ipr-enforcement/

New legislation in the country of Denmark
https://www.teliacompany.com/en/news/news-articles/2017/danish-legislation/

On data retention legislation in Sweden
(*In Swedish*) http://press.telia.se/news/datalagringsfraagan-vi-behoever-en-lagstiftning-som-tillgodoser-saavaelbehovet-av-brottsbekaempning-som-behovet-av-integritet-210198?utm_source=rss&utm_medium=rss&utm_campaign=Subscription&utm_content=news

LAWS PROVIDING GOVERNMENTS DIRECT ACCESS

When it comes to governments' direct access, i.e. signals intelligence (intelligence gathering through analysis and processing of communication signals) and real-time access without requests (technical systems for more extensive monitoring of telecommunications), Telia Company has no insight into the extent of such surveillance and cannot provide any statistics.

What Telia Company can do is publish a list with links to such legislation in all of our respective markets. The list shows that in most of our geographies the state has implemented such a power.

First and foremost, it is important to note that detailed legal and administrative frameworks for surveillance often remain classified, and little is public about the ways in which captured data are operationalized. The systems and regulations vary from country to country. They apply to all operators in each respective country.

It is our view that, while there may be legitimate public-interest reasons for maintaining the secrecy of technical and operational specifications, generic information about the nature and extent of surveillance should be made available to the public. Without such information, it is impossible for rights holders to assess the legality, necessity, and proportionality of these measures. States should therefore be transparent about the use and scope of communications surveillance.

In accordance with our freedom of expression policy, Telia Company advocates that governments should not have direct access to a company's networks and systems. Telia Company should retain operational and technical control. Telia Company also advocates clear and transparent legal provisions on proportionality and necessity for all government surveillance of communications. Vague, non-transparent, and broadly conceived legal provisions are not appropriate when freedom of expression is at stake. Telia Company's views are reflected in the blog 'Direct Access systems and the right to privacy', published by the Freedom Online Coalition.

> The United Nations, in its Resolution on the 'Promotion, protection and enjoyment of human rights on the Internet'from June 2016: (1)
>
> " 8. Calls upon all States to address security concerns on the Internet in accordance with their international human rights obligations to ensure protection of freedom of expression, freedom of association, privacy and other human rights online, including through national democratic, transparent institutions, based on the rule of law, in a way that ensures freedom and security on the Internet so that it can continue to be a vibrant force that generates economic, social and cultural development. "

Surveillance includes both real-time interception and historical data. While systems for direct access normally provide real-time access to communications, such systems normally do not provide access to historical data. Governments, also those with direct access to a company's networks and systems, thus normally turn to operators with requests for historical data.

Telia Company has below listed the most relevant laws on;

- Signals intelligence, i.e. intelligence-gathering through analysis and processing of communication signals; and/or
- Real-time access without requests, i.e. technical systems for more extensive possibilities to monitor telecommunications.

(1) http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/32/L.20

Azerbaijan	The Constitution of Azerbaijan Republic (the main law). Art. 32.4. http://en.president.az/azerbaijan/constitution Detective-Search Activity Act of the Republic of Azerbaijan. Art.10; 11; 12. The Law on Telecommunication, Art. 39. Related Decrees of the President of Azerbaijan Republic: a) Dated 19.06.2001; N-507 b) Dated 01.06.2015; N-539 c) Dated 02.10.2015; N-639 Main laws http://www.e-qanun.az/code/14 http://www.e-qanun.az/framework/10663 http://www.e-qanun.az/framework/2938 http://www.e-qanun.az/framework/897 http://www.e-qanun.az/framework/19675 Main decrees http://www.e-qanun.az/framework/3569 http://www.e-qanun.az/framework/36369 http://www.e-qanun.az/framework/34887 http://www.e-qanun.az/framework/30840
Denmark	No signal intelligence and/or real-time access without requests in the legislation with the exception of that the Center For Cybersecurity may initiate lawful interception without a court order, but only if companies or governmental authorities have signed up for or requested this ad hoc. Telia Denmark is not a party to this arrangement and does not allow lawful interception without a court order.
Estonia	Electronical Communication Act (Elektroonilise side seadus) https://www.riigiteataja.ee/en/eli/521082017008/consolide The relevant section is § 113 in Chapter 10
Finland	In January 2018, the Finnish Government proposed new civilian and military intelligence legislation. The proposals outline that the authorities will not have a direct and unlimited access to all network traffic. The government's proposals can be found in here: https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_198+2017.aspx (proposal on amendment of the constitution) https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_199+2017.aspx (proposal on oversight of intelligence gathering) https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_202+2017.aspx (proposal on civilian intelligence) https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_203+2017.aspx (proposal on military intelligence)
Georgia *NB: In Georgia the only way to access a correct and up-to-date version of the act is through the paid subscription site www.matsne.gov.ge*	Law of Georgia on Personal Data Protection *Art. 2, paragraphs U, V, W Art. 35(1) Art. 55(1)* http://personaldata.ge/en/legislation/national-legislation Criminal Procedure Code of Georgia, parts *parts 31, 32, 33 of Art 3, Art. 143(1) -143 (10), Art. 332(3)* https://matsne.gov.ge/ka/document/view/90034 Law of Georgia on Electronic Communications *definitions h(56) – h(62) of Art 2,, Art. 8(1), 8(2) and 8(3)* https://matsne.gov.ge/ka/document/view/29620 Law of Georgia on State Secrecy, *Art. 7, paragraph 4, sub-paragraph "a"* https://matsne.gov.ge/ka/document/view/2750311
Kazakhstan	Law on National Security, Art. 23: http://adilet.zan.kz/rus/docs/Z1200000527 Law on Communication, Art. 8.1.17; Art 15, Art 21.3 http://adilet.zan.kz/rus/docs/Z040000567_ Law on Operative Investigative Activities, Art 11: http://adilet.zan.kz/rus/docs/Z940004000_ Law of Criminal Procedure, Articles 231 – 245 *http://adilet.zan.kz/rus/docs/K1400000231*
Latvia	The Electronic Communication Law (http://likumi.lv/doc.php?id=96611), Section 69 "Connection to Electronic Communications Networks"

	Cabinet of Ministers regulations No Nr.591 “Procedure for equipping electronic communication network for obtaining investigatory information from technical equipment and investigatory wiretapping of conversations in the cases specified by law” (unofficial translation). Original language document: http://likumi.lv/doc.php?id=114208
Lithuania	Criminal Code of the Republic of Lithuania: https://www.e-tar.lt/portal/lt/legalAct/TAR.2B866DFF7D43/ZpNMZQSaRN Code of Criminal Procedure of the Republic of Lithuania: https://www.e-tar.lt/portal/lt/legalAct/TAR.EC588C321777/RKDzuhQANj Law on Criminal Intelligence of the Republic of Lithuania: https://www.e-tar.lt/portal/lt/legalAct/TAR.3B8E4F16C815/hxVVzGWbGr Law on Intelligence of the Republic of Lithuania: https://www.e-tar.lt/portal/lt/legalAct/TAR.1881C195D0E2/XYOnFcTdIT
Moldova	Art. 20 of the Law on electronic communications: http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=327198 Art. 132 Criminal Procedure Code: http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=350171 Art. 7 of the Law on Intelligence Security Service: http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=311721 Art. 18 of the Law on special investigation activity: http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=343452
Norway	According to the Criminal Procedure Act: https://lovdata.no/dokument/NL/lov/1981-05-22-25 According to the section 6-2a Electronic Communication Act, the police may use frequencies allocated to others through the use of “mobile restricted zones”. This cannot be done without a court decision. The police should also notify the National Communication Authority (NCA) without undue delay after the measure has been established. https://lovdata.no/dokument/NL/lov/2003-07-04-83
Sweden	Law on Defence Intelligence http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2008717-om-signalspaning-i_sfs-2008-717 Additional information. www.fra.se / Om FRA / Lagstiftning
Uzbekistan	Presidential Decree 513 On measures to increase effectiveness of organization of operative investigation measures on telecommunication networks (See document nr 8 under Section 3) https://nrm.uz/contentf?doc=438910_polojenie_o_poryadke_organizacii_ispolzovaniya_tehnicheskih_sredstv_sistemy_operativno-rozysknyh_meropriyatiy_na_setyah_telekommunikaciy_respubliki_uzbekistan_(prilojenie_k_postanovleniyu_prezidenta_ruz_ot_21_11_2006_g_n_pp-513)&products=1_vse_zakonodatelstvo_uzbekistana Law on Telecommunications, Art. 18: http://www.lex.uz/Pages/GetAct.aspx?lact_id=33152

Telia Company owns and operates one of the largest fiber-optic networks in the world, ‘Telia Carrier’, providing network infrastructure and services to more than 1,000 customers in 80 different countries worldwide. These markets have not been included in the above list of laws regarding signals intelligence and direct access. It is worth noting that there are markets in scope of Telia Carrier which have that type of direct access legislation, such as Germany and Hungary.

In addition, Telia Company has a minority ownership in Turkcell (Turkey) and, until October 2017, had a minority ownership in Megafon (Russia). Here added, therefore, a list of the most relevant laws regarding what we interpret as direct access signals intelligence and real-time access without requests in Russia and Turkey;

Russia	Federal law № 144-FZ dated August 12, 1995 “On investigative activity” (unofficial version) http://www.legislationline.org/documents/action/popup/id/4191 Federal law № 126-FZ dated July 07, 2003 “On communications” (unofficial version) http://telecomlaw.ru/eng/legislation/legislation.html Rules approved by decree of the Government of the Russian Federation № 538 dated

	August 27, 2005 “Rules of cooperation” (No link available) Law No:5271 on Criminal Procedure Code (No link available)
Turkey	Law No: 5271 on Criminal Procedure Code Law No: 5809 on Electronic Communications Law No: 2559 on Duties and Powers of the Police Law No: 2803 on the Organization, Duties and Powers of the Gendarmerie Law No: 2937 on State Intelligence Services and National Intelligence Organization Law No: 5651 on Regulating Online Content and Tackling Crimes Committed via Online Content Law No: 7091 on State of Emergency Safeguards (All of the above laws available via www.mevzuat.gov.tr

Publishing the above links to laws on signals intelligence and real-time access without requests only does part of the job. In Telia Company’s view, customers should have easily accessible and user-friendly information on all surveillance legislation. In the same way as regards statistics on the extent of surveillance, it is of course at first Governments who are to provide citizens with information about surveillance legislation. Telia Company and other players can, however, undertake to help make this information more accessible. This is why the Telecommunications Industry Dialogue elaborated a database covering, to date, 51 countries describing some of the most important surveillance powers available to government agencies and authorities seeking access to customer communications. Most of the information in the database was provided by Vodafone and Telenor. The work, now continued within the Global Network Initiative (GNI), of which Telia Company is an active member, includes reports on Denmark, Norway, Kazakhstan, Russia, Sweden and Turkey. We hope the database is useful to civil society organizations, academics, investors, and others who study the norms regulating government access to communications and their capacity to restrict content. Telia Company’s aim is to continue to help building on this joint resource.

The database with information on surveillance legislation in, presently, 51 countries is available here; http://globalnetworkinitiative.org/legalframeworks

LAWS ON MANDATORY DATA RETENTION FOR LAW ENFORCEMENT

The European Court of Justice (ECJ) in December 2016 (Joint Cases C-203/15 and C-698/15) concluded that EU law constitutes a barrier to national legislation which, for law enforcement, provides for general and undifferentiated storage of all traffic data and location data for all subscribers and registered users and all electronic means of communication.

Legislation on mandatory data retention by companies for law enforcement is in scope of this report on law enforcement disclosure. Telia Company therefore here provides a list of applicable laws in our markets.

Azerbaijan	Law on Telecommunication. Art. 48.4 and 48.5. http://www.e-qanun.az/framework/10663 Law on Private Information. Art. 7. and art.9. http://www.e-qanun.az/framework/19675
Denmark	BEK nr. 988 28/9-2006 with amendments: "Executive order on Data Retention"
Estonia	Electronic Communication Act (Elektroonilise side seadus) https://www.riigiteataja.ee/en/eli/521082017008/consolide The relevant section is §111[1] in Chapter 10
Finland	Information Society Code, section 157 https://www.finlex.fi/en/laki/kaannokset/2014/en20140917.pdf
Georgia	Operators are not obliged to retain data, however this obligation lies with the authorities.
Kazakhstan	http://adilet.zan.kz/rus/docs/Z040000567_
Latvia	The Electronic Communications Law (https://likumi.lv/ta/id/96611), Section 71.1 "Utilization and Processing of Data to be Retained" Cabinet of Ministers Regulation No 820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled" (https://likumi.lv/ta/id/167539)
Lithuania	Law on electronic communications of the republic of Lithuania https://www.e-tar.lt/portal/lt/legalAct/TAR.82D8168D3049/NgcguIkcSk
Moldova	Law on electronic communications of Republic of Moldova, art. 20 p. 3): http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=372518; Law on prevention of cybercrimes, art. 7 p. b) about data preservation: http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=333508
Norway	None
Sweden	None. Telia Sweden article December 30th 2016 (In Swedish); 'The data retention issue – We need legislation which meets both the need to fight crime and the need for privacy' http://press.telia.se/news/datalagringsfraagan-vi-behoever-en-lagstiftning-som-tillgodoser-saavael-behovet-av-brottsbekaempning-som-behovet-av-integritet-210198
Uzbekistan	None
Russia	Federal Law N 374-FZ, from July 6th 2016. The majority of the amendments came into effect on July 20th, 2016. Some of the requirements relating to storage of metadata, however, will only come into force starting from July 1st, 2018. Order, terms and volumes of storage should be specified by the Government (drafts of relevant regulations/by-laws are considered).
Turkey	Data retention rules are disseminated in each of the below mentioned laws; Law No: 5271 on Criminal Procedure Code Law No: 5809 on Electronic Communications Law No: 2559 on Duties and Powers of the Police Law No: 2803 on the Organization, Duties and Powers of the Gendarmerie Law No: 2937 on State Intelligence Services and National Intelligence Organization Law No: 5651 on Regulating Online Content and Tackling Crimes Committed via Online Content Law No: 7091 on State of Emergency Safeguards (All of the above laws available via www.mevzuat.gov.tr

GOVERNMENT LAW ENFORCEMENT DISCLOSURE REPORTS

We encourage governments to be transparent about their use and scope of surveillance of communications. We welcome reports where the respective government regularly and publicly report to their Parliament about the scope of surveillance. Although these publications might not always cover all kinds of requests and demands, we see government reports as the preferred starting point for discussing best practices for meaningful transparency. Each government can cover all telecom operators in any respective country, and can also best respond to any questions regarding proportionality of surveillance.

Law Enforcement Disclosure Reports from Governments;

Denmark:
http://anklagemyndigheden.dk/sites/default/files/inline-files/statistik-over-indgreb-i-meddelelseshemmeligheden-og-ransagninger-2016.pdf

Finland:
http://intermin.fi/kertomukset-ja-selvitykset

Georgia:
Link provided by the Georgian Data Privacy Office:
http://www.supremecourt.ge/statistics/2017/

Lithuania:
Telia Company and Telia in Lithuania have not been granted permission to publish statistics regarding how many requests we have received in Lithuania, except for statistics as regards lawful interception.

We welcome, however, that Lithuania like many of the other countries publishes its own statistics in reports from the Lithuania State Security Department. The data is grouped together with other activities, such as access to homes. The latest report for 2016 (page 8) states: “In 2016 VSD has performed 2026 actions sanctioned by the district courts, and mostly the information transmitted through electronic communications networks was captured. In total, actions were carried out against 1948 legal and natural persons. The court sanctioned actions were carried out in respect of 874 citizens of the Republic of Lithuania, 1040 in relation to foreign citizens and 34 in relation to legal persons. .”
https://www.vsd.lt/wp-content/uploads/2016/10/2016_veiklos-ataskaitaVIESA_0330.pdf

There is also a report from the Lithuanian State Security Department, in Lithuanian. In 2015 VSD activities authorized by courts were carried out against 1953 individuals – 1017 Lithuanian citizens, 904 foreign nationals and 32 legal persons. In most cases, the transmission of information in electronic communications networks were monitored.
https://www.vsd.lt/wp-content/uploads/2016/10/Veiklos-ataskaita-2015.pdf

Norway:
http://sivilrett.custompublish.com/get-file.php/3925898.2254.aaiinizt7atbzz/%C3%85rsrapport+2016.pdf and
https://eos-utvalget.no/norsk/arsmeldinger/content/text_1401199471784/1491375612710/aarsmelding2016no.pdf

Sweden:
http://data.riksdagen.se/dokument/H50369.html
and additional reporting
http://www.sakerhetspolisen.se/ovrigt/pressrum/aktuellt/aktuellt/2017-06-02-redovisning-av-anvandningen-av-hemliga-tvangsmedel-under-2016.html

ADDITIONAL TRANSPARENCY

Publicly sharing Telia Company's tool for assessing and escalating unconventional authority requests

Telia Company regards unconventional requests and demands from authorities which might potentially have serious impacts on the freedom of expression in telecommunications, as 'major events'. These are requests or demands regarding, for instance, mass surveillance initiated by national security authorities, shutting down of networks, the blocking or restricting of access to telecom services or networks, or initiatives for new law-making which might potentially have serious impacts on freedom of expression and privacy.

Within Telia Company, such unconventional requests and demands are intended to be assessed and escalated in a way so that locally, regionally and group-wide, Telia Company can seek ways to respect freedom of expression and privacy. An internal tool for assessing and escalating has been elaborated and updated, based on learnings from actual major events, since the adoption by Telia Company of the freedom of expression policy. We seek, in this way, to contribute to industry best practice of shared learning.

The purpose of sharing the tool is to globally support implementation and further development of industry best practices, to promote and respect freedom of expression within the in ICT industry, and to aim for practical measures on the ground with regard to the freedom of expression of customers and users.

We also want to open up our tool for rights holder representatives and other stakeholders to comment upon our approach to help build the best possible process together.

The latest version of Telia Company's Form is available here; The Form has also been made available by the industry organization GSMA in its policy handbook for handling of service restriction orders, here.

Requests for mass-sms's in Uzbekistan

In some of our markets, operators are requested to send messages (e.g. SMSs) to customers on behalf of the government. The below example illustrates how this can look like.

During 2017 Telia Company's local company in Uzbekistan, Ucell, received 24 number of requests for bulk-SMS's to its customers, three of these were rejected by Ucell. These mass-sms requests have all been mandatory based on the Ucell applicable license agreement. The mass-sms's have not been politically motivated but part of the Ucell social contribution scope. Each SMS has included information on which Authority that was the sender. These SMS's have not been of an unconventional nature in relation to the freedom to seek and receive information. Mass-sms's sent during 2017 were such as "*Dear citizens, actively participate on Saturday's and Sunday's in the 'Day of Purity' events! Hokimiyat*"; "*Dear subscriber! The old passport must be replaced until June 2018. Upon renewal, update the passport data in one of offices of Ucell. MVD RUz*."; "*Dear taxpayers! Do not forget to pay property tax and land tax from individuals until October 15, 2017! STC of RUz*"; and "*For the prevention of botulism, do not cook or consume canned foods cooked at home. Ministry of Health.*"

QUESTIONS AND ANSWERS

Why is Telia Company publishing these reports?
Like all telecommunication operators, we are required by laws in the countries within which we operate to assist authorities for purposes such as enforcing criminal law. We are only to disclose customer information in accordance with the law and we insure the process to ensure it complies with the law.

By publishing Law Enforcement Disclosure Reports we want to make sure that our customers have access to information about that, and to what extent, government authorities have the power to access data based on law and that Telia Company, according to our policies and procedures, protects customers. Our instruction include to provide data to authorities only if and to the extent required to do so. We also point out and link to legislation which render the governments in most of our markets direct access to our systems and networks as well as links to national laws on mandatory data retention for law enforcement purposes.

We encourage governments to be transparent about their use and scope of surveillance of communications. Telia Company's advocacy is based on our Group Policy on Freedom of Expression Policy and Surveillance Privacy, available here .

Do you ever challenge a request?
At Telia Company, requests from law enforcement authorities are handled by specially set-up units that have been trained to handle these requests according to the processes in place. All requests from authorities must be legally correct. Telia Company is to reject or challenge 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. In such cases, the process is for Telia Company to ask for clarification.

As to unconventional government requests ('major events'), according to our Group Policy on Freedom of Expression and Surveillane Privacy, we have committed to and determined how to pursue a point-of-challenge when our customers' freedom of expression and surveillance privacy is at risk. This implies that we are to make careful assessments of all unconventional requests and demands that may have serious impacts on freedom of expression or surveillance privacy. A strict escalation procedure for internal decision-making has been put in place to follow the policy. Formal decisions on the extent of compliance or push-back following problematic requests or demands are not to be made at local company level alone, unless there are exceptional reasons.

Why do the figures differ between countries?
Several factors make it difficult to compare the law enforcement disclosure statistics between countries. Telia Company has different market-shares in different countries, which is probably reflected in the figures. Furthermore, Telia Company is privy to each local authorities' working-methods and priorities in different countries, and these methods are likely to differ. Different demands from authorities result in different working-methods in different countries. We work to align reporting.

It is also important to note that the figures show the number of requests from authorities, not the number of individuals that have been targeted. Not even Telia Company as the operator and provider of the information has this knowledge. The number of requests is most likely larger than the number of individuals that have been targeted. Also, in some countries, one request may include several targets.

Does Telia Company make money on this?
No. Local legislation often prescribes that the operators must finance the system setup and that the authority has to compensate for every single request (cost-based).

How might these reports be used?
Telia Company's aim is to make it transparent to users and stakeholders to what extent governments' access customer data. Our Law Enforcement Disclosure Reports might help getting a clearer picture of the norms governing surveillance. The reports might therefore be useful in research and advocacy. We also encourage governments to be transparent about their use and scope of surveillance of communications.

How does Telia Company enforce its Policy and internal instruction and processes in this context?
Our Policy is included in relevant employee training, and also in our whistle-blowing mechanism (the Telia Company 'Speak-Up Line'). The Policy is part of our internal oversight and accountability model. Telia Company has also conducted Human Rights Impact Assessments, followed by action plans and prioritizations.

Has Telia Company a grievance mechanism in place, open for grievances regarding freedom of expression and privacy?
Yes. Telia Company's grievance mechanism, our 'Speak-Up Line', is applicable and available here.

Does Telia Company inform its users when their data has been revealed to authorities?
No. It is generally defined by legislation if and when the requesting authority shall inform the user about the surveillance conducted by the authority.

What are the main challenges associated with Law Enforcement Disclosure Reporting?
It should be noted, within the context of this report, that governments also have direct access, i.e. signals intelligence and real-time access without sending requests to the operators. Regarding 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 such legislation in our respective markets, in the way we do in this report.

Telia Company

Telia Company AB (publ)
Corporate Reg. No. 556103-4249,
Registered office: Stockholm
Tel. +46 8 504 550 00. www.teliacompany.com