TELIA COMPANY LAW ENFORCEMENT DISCLOSURE REPORT 2022

CONTENTS

Executive summary

This Law Enforcement Disclosure Report aims to offer detailed and updated insights into the context and extent of surveillance and collection of customer data by governments and authorities in Telia Company's markets. The report includes statistics on typically lower risk so called conventional (day-to-day) authority requests, information on legislation regarding 'direct access' and on mandatory 'data retention' for law enforcement purposes. It also includes information on unconventional authority requests which Telia labels "major events" since they might potentially be associated with high risks to the rights of individuals.

A summarized version of this report is published in the Telia Company 2022 Annual and Sustainability Report available at annualreports.teliacompany.com which is externally assured by Deloitte. This full report provides more context, as well as information about definitions, challenges, and the scope of the reporting.

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.

Safeguarding privacy is of utmost importance at Telia: It is one of the pillars of our Code of Conduct. At the same time, Telia 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.

"Safeguarding privacy is of utmost importance at Telia: It is one of the pillars of our Code of Conduct."

According to our policies and procedures, Telia discloses information to authorities only when required by law and only to the extent required by law. This is a non-negotiable part of the way we are to operate. Our process is intended to identify and mitigate potential violations to individuals' freedom of expression and privacy, and we have clear escalation procedures in place to make sure that risks to these rights are handled in a robust way. However, it is important to stress that the actual outcome of such as information requests heavily depends on local laws. Governments in most of our markets also have direct access, where Telia has no insight into the extent of surveillance (when, who and what) and cannot provide statistics. What we can do, as in this report, is to be transparent about the laws applicable in the markets where we operate. We also provide links to laws on mandatory data retention for law enforcement purposes, as well as to take-down as defined by law of terrorist content online.

The issues can be complex. Different stakeholders have different views on topics related to freedom of expression and privacy, 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 privacy, even as we accept that sometimes there need to be limitations on those rights, to the extent allowed by applicable legislation. Limitations – defined by governments - must be necessary and proportionate and clearly delineated within a strong legal framework, with the right checks and balances. Whenever there is an opportunity, we argue for legislation which supports and promotes freedom of expression and privacy.

We encourage governments to be transparent themselves about their use and scope of surveillance of communications. We welcome reports – such as the ones in Denmark, Finland, Lithuania, Norway, and Sweden – where each respective government regularly and publicly reports about the scope of their surveillance, even if these publications might not always cover all types of requests and demands. We view such publicly shared government reporting as the preferred starting point for meaningful transparency, based on the fact that a government can cover not only Telia but all operators in any respective country, and that a government can also respond to any questions as to the actual necessity and proportionality of the surveillance and other measures they apply.

To supplement such government reporting we publish our Law Enforcement Disclosure Report together with our Annual and Sustainability Report every year in March. The report covers conventional day-to-day requests from the police and other authorities in Denmark, Estonia, Finland, Lithuania, Norway, and Sweden. We also publish information about unconventional requests, i.e. 'major events'. In 2022, major events related to such as blocking of specific content on the Internet and removal of TV-stations from Telia TV services, but also new legislation on take-down of content on the Internet, use of anonymized and aggregated data to fight corona, and a significant imposed operational change for blocking of content on the Internet. Additional information about those requests can also be found on our website.

Solna March 13th, 2023

Stefan Backman
Group General Counsel

1. ABOUT THIS REPORT

Purpose of the report

Telia Company is committed to respect freedom of expression and the privacy of our users. This report reflects that ambition and aims 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 can do is to challenge such requests if they have no or unclear legal grounds, advocate for necessity and proportionality and inform its customers and stakeholders of the extent of such surveillance, including the legal context. Through this our transparency reporting in the context of surveillance and content restrictions, we aim to build user trust and gain the confidence of investors and other stakeholders by demonstrating that Telia manages its human rights risks related to freedom of expression and privacy in a proper way. Our aim is also to contribute to meaningful oversight and discussions regarding the proper limits of government powers in this context.

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

Statistics on conventional requests as well as information on unconventional requests during 2022 have undergone limited assurance as part of the Annual and Sustainability Report assurance process. See Appendix 1 for the information included in the Annual and Sustainability report.

What we report

We have published Law Enforcement Disclosure Reports since 2014. Through this our transparency reporting in the context of surveillance and content restrictions, we aim to build user trust and gain the confidence of investors and other stakeholders by demonstrating that Telia manages its human rights risks related to freedom of expression and privacy in a proper way. Our aim is also to contribute to meaningful oversight and discussions regarding the proper limits of government powers in this context.

In this report, we provide:

- Statistics on the number of *conventional* ('day-to-day') law enforcement requests reported in four different categories; 'Lawful interception', 'Historical Data', 'Subscription Data' and 'Challenged/rejected requests'
- Information about *unconventional* ('major events') government requests and legislative initiatives; and
- Links to laws providing governments with direct access, links to laws on mandatory data retention for surveillance, as well as to the EU Regulation on terrorist content online.

The governments' requests can be divided into four main categories:

Category 1**: Requests from law enforcement authorities:**
1.a) 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)
1.b) Real-time access to traffic data (e.g. checking who is calling who, when and for how long or internet traffic)
1.c) Access to historical traffic data which the provider has stored or retained (e.g. checking who has called who, when and for how long)
1.d) Access to subscription data which the provider has stored or retained (e.g. checking who is the subscriber of a certain telephone-number)
1.e) 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)
1.f) Requests to block content online
1.g) Requests for takedown of terrorist content online

Category 2**: Signals intelligence:** i.e. intelligence-gathering through analysis and processing of communication signals (example: the Swedish National Defense Radio Establishment/Försvarets Radioanstalt).

Category 3**: Direct access without requests:** Real-time network access without requests, i.e. signals intelligence (intelligence gathering through analysis and processing of communication signals) and technical systems for more extensive monitoring of telecommunications.

Category 4**: Shutdown, blocking, restriction of access, etc. ('unconventional requests and demands').** Examples: Shutdown of communications, shutdown of internet access, blocking of websites or demands to install or upgrade systems for direct access.

How we report

Reporting on Category 1: Telia Law Enforcement Disclosure Reporting on statistics. See section 3. From March 2019, we report on the extent of blocking requests, see section 8. From 2022 onwards we also report on the application of the EU Regulation on terrorist content online, see section 6.

Reporting on Categories 2 and 3: Telia has no insight into the extent of surveillance and cannot provide any statistics. Telia has, however, added a list of national legislation within these two categories to this report, see section 4. Proposals for new laws or significant, imposed operational changes in the area of these two categories may be defined as unconventional requests ('major events') within the below Category 4.

Reporting on Category 4: Telia reporting on unconventional requests and demands ('major events'). See section 2.

Challenges and scope

We here aim to give readers the possibility to understand our main reporting challenges and omissions and make their own judgments.

Conventional requests

Several aspects and limitations make it challenging to compare information over time as well as between markets. For more information, see Appendix 2.

Unconventional requests

There are several challenges related to transparency on unconventional requests. Local laws determine what can be published. There may be confidentiality provisions and/or constraints based on our duty to protect the safety of our employees. Furthermore, issues regarding direct access are closely related to national security and are therefore complex and challenging to communicate. Also, counting the number of unconventional requests can be difficult and subjective as they can range from demands to block one or several websites or shutting down a network locally, to requests regarding direct access.

Out of scope for this report

Non-surveillance requests

Telia's statistics do not include requests from authorities that have no role in lawful interception, nor other services to which operators are obliged to adhere to such as requests from competition authorities, from national regulatory authorities or requests based on the EU copyright IPR Enforcement Directive. Also, the report does not cover information on Telia's voluntary commitment to block child sexual abuse material based on a list from either 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 call to the local emergency number. We have, however, placed manual positioning requests, which are mostly conducted in relation to rescue efforts, in the 'Historical data' category.

Privacy and data protection

This report covers Telia's commitments to freedom of expression and surveillance privacy and our interaction with law enforcement authorities. How we work with data for operational and commercial purposes is not covered in this report but defined in our Policy 'Privacy and Data Protection', available here and in our Annual and Sustainability report.

Requests or demands from private entities

Telia's local companies are not to act upon requests or demands from private entities to remove, filter or restrict access to content – unless mandated by a court or authority to do so. Telia, however, actively participates in combating spam, viruses and distributed denial of service (DDoS) -attacks to protect our customers and networks.

2. UNCONVENTIONAL REQUESTS AND DEMANDS

Telia regards unconventional requests and demands from authorities which might potentially have serious impacts on the freedom of expression and privacy of individuals 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 privacy defines Telia's commitments in relation to such unconventional requests or demands with potentially serious impacts on freedom of expression and privacy, such as shutdown of networks and blocking of access to the Internet or specific websites. We also include and address as 'major events' such requests in the context of freedom of expression and privacy which are not based on law, as well as initiatives for new law-making and significant imposed or proposed operational changes which might potentially have serious impacts on freedom of expression and privacy. In this category we also include requests and demands to install or upgrade 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. There are, however, several challenges related to transparency on unconventional requests. Local laws sometimes lack full clarity determining what can be published. There may be strong confidentiality provisions and/or constraints based on our duty to protect the safety of our employees. With regards to direct access the topic is closely related to national security and is therefore complex and challenging to communicate.

Below we publish the number of unconventional requests received during the year. Please note that the numbers are somewhat arbitrary. If in one country a large number of websites were requested to be blocked as part of one request, and in another country only one, then each of these two counts as one request in the figures below. A shutdown of the network or a service in *a limited part* of a country would be counted as a major event equal to a shutdown of the network or service in *all* of a country. A minor update of a system for government direct access to Telia's networks and services is counted equally to a much more substantial upgrade of such a system. Etcetera.

Unconventional government requests are assessed by the local company and escalated to Group level for informed joint decision making, including considerations from outside of the local context, and, if required, support 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 the requesting Authority or Government that a decision be put in writing 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 and sometimes also the ability to act under the local circumstances.

Telia also contributes to external reporting of unconventional requests in the public assessment report of multi-stakeholder initiative Global Network Initiative (GNI), latest published in April 2020, see pages 16-18 here.

Unconventional requests and demands during 2022

During 2022, we closed some 15 unconventional requests and demands across our markets. See further details in Appendix 1.

Unconventional requests and demands during 2021

During 2021, we closed almost 20 unconventional requests or demands across our markets. To ensure consistency, group-level experts facilitated local assessments and escalations. Requests included proposals for new legislation, blocking of content or services, mass surveillance, and requests for voluntary measures. In more than 80% of cases, Telia took some kind of measure to promote freedom of expression and surveillance privacy or mitigate risks in some way, through for example comments to the lawmaker, transparency, appeal of court decision, or asking for the rule of law to apply declining to act on a voluntary basis. Such actions were defined jointly by local companies and representatives of Group Executive Management.

Unconventional requests and demands during 2020

During 2020, we closed close to 20 unconventional requests or demands across our markets. To ensure consistency, group-level experts facilitated local assessments and escalations. Requests included such as new legislation, blocking of content, and requests for voluntary measures. Around one third of the requests were COVID-19 related. In around three out of four cases, Telia Company took measures to promote freedom of expression and surveillance privacy in some way, through for example comments to the lawmaker, transparency, appeal of court decision, or asking for the rule of law to apply. Such measures were defined jointly by local companies and representatives of Group Executive Management. When it is possible to be transparent on some or all relevant information as to a specific unconventional request, Telia Company does so by also publishing articles on www.teliacompany.com During 2020, such articles have been on COVID-19 related requests from authorities throughout all our markets, with an article published in April followed by regular updates, the latest one in December, available here. Telia Company also contributes to external reporting of unconventional requests in the public assessment report of multi-stakeholder initiative Global Network Initiative (GNI), published in April 2020, see pages 16-18 here.

Unconventional requests and demands from 2013 to 2019

Please see our earlier reports, available here.

3. STATISTICS FOR CONVENTIONAL REQUESTS

The statistics for conventional authority requests 2020, 2021 and 2022 is provided in Appendix 1.

The figures show the number of day-to-day conventional requests from authorities, not the number of individuals to whom they relate. To facilitate comparison over time, previous year's figures have been included.

Several factors make it difficult to compare statistics between countries. Telia has different market shares in different countries, which is likely reflected in the figures. Telia does not have knowledge of the authorities' working methods and priorities in different countries, but the methods are likely to differ. Within the group, there are different internal methods of collecting data in different local operations, causing certain variations of reported data. As noted, the figures show the number of requests from authorities, not the number of individuals concerned. Not even we as the operator and provider of the information to the authorities have this knowledge. Most likely, in the category of lawful interception, the number of requests is larger than the number of individuals concerned.

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), however, the number of affected individuals will naturally be larger than the number of requests. Depending on the scope of such a request, Telia is required to hand out varying amounts of customer data. The amount 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 normally naturally higher. 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 requests separately, but in the Nordics we have usually and over time received roughly around 50 to 100 cell tower dump requests per 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.

For more information about definitions, data sources and main challenges, see Appendix 2.

For statistics before 2020, please see our page for Law Enforcement Disclosure reports here.

4. LAWS PROVIDING GOVERNMENTS DIRECT ACCESS

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

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 capturing of data is operationalized. The systems and regulations vary from country to 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 rightsholders to assess the legality, legitimacy, necessity, and proportionality of these measures. States should therefore be transparent and clear about the use and scope of communications surveillance.

In accordance with our policy on freedom of expression and surveillance privacy, Telia advocates that governments should not have direct access to a company's networks and systems. Telia should retain operational and technical control. Telia 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 and surveillance privacy is at stake. Telia's views are, since long, reflected in the blog 'Direct Access systems and the right to privacy', published by the Freedom Online Coalition.

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 having direct access to a company's networks and systems, thus normally in parallel turn to operators with requests for historical data.

Below we list the most relevant laws in the markets where we operate (as of March 2023) with regards to;

- 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.

Denmark

The Centre For Cyber Security under the Defense Intelligence Service may install monitoring equipment at operator premises to monitor traffic to and from company addresses (not monitoring of customer networks) for the purpose of discovering cyber-attacks against operators. The installation is voluntarily and Telia Denmark is not a party to this arrangement.

Act on Center For Cyber Security: https://www.retsinformation.dk/eli/lta/2019/836

Estonia

Electronical Communication Act ('Elektroonilise side seadus'):
https://www.riigiteataja.ee/en/eli/ee/521082017008/consolide/current The relevant section is in Chapter 10.

Finland

Act on military intelligence: http://finlex.fi/fi/laki/ajantasa/2019/20190590
Act on civil intelligence: http://finlex.fi/fi/laki/ajantasa/2019/20190582
Police Act (section 5 a): https://www.finlex.fi/fi/laki/ajantasa/2011/20110872

Latvia

The Electronic Communication Law: (Elektronisko sakaru likums (likumi.lv)), Section 96 “Connection to Electronic Communications Networks”.
Operational Activities Law: https://likumi.lv/ta/en/en/id/57573-operational-activities-law
Criminal Procedure Law: https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law

Lithuania

Criminal Code of the Republic of Lithuania:
https://www.e-tar.lt/portal/lt/legalAct/TAR.2B866DFF7D43/asr
Code of Criminal Procedure of the Republic of Lithuania:
https://www.e-tar.lt/portal/lt/legalAct/TAR.EC588C321777/asr
Law on Criminal Intelligence of the Republic of Lithuania:
https://www.e-tar.lt/portal/lt/legalAct/TAR.3B8E4F16C815/asr
Law on Intelligence of the Republic of Lithuania:
https://www.e-tar.lt/portal/lt/legalAct/TAR.1881C195D0E2/asr
https://www.e-tar.lt/portal/lt/legalAct/TAR.1881C195D0E2/asr

Norway

Criminal Procedure Act: https://lovdata.no/dokument/NL/lov/1981-05-22-25

According to section 6-2a of the 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

The Norwegian Parliament in 2020 adopted a proposal for a new intelligence act. The new legislation requires telecom providers to facilitate that the Norwegian Intelligence Service can access data in their network which crosses national borders. The legislation available in Norwegian here: https://www.regjeringen.no/no/aktuelt/ny-etterretningstjenestelov-er-vedtatt-i-stortinget/id2705969/

Sweden

Law on Defense 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

5. LAWS ON MANDATORY DATA RETENTION FOR LAW ENFORCEMENT

Legislation on mandatory data retention by companies for law enforcement is in scope of this report since it is an obligation on operators which impacts the privacy of individuals. Telia therefore provides a list of laws applicable in our markets.

It should be noted that 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.

Denmark

Act on electronic communications network and services: https://www.retsinformation.dk/eli/lta/2022/955

Executive Order No. 381 29/3-2022 on general and undifferentiated logging until 29 March 2023 and storage until 29 March 2023 of traffic data: https://www.retsinformation.dk/eli/lta/2022/381

Estonia

Electronic Communication Act ('Elektroonilise side seadus'):
https://www.riigiteataja.ee/en/eli/ee/521082017008/consolide/current The relevant section is in Chapter 10.

Finland

Act on Electronic Communications Services (917/2014), section 157 (formerly Information Society Code):
https://www.finlex.fi/en/laki/kaannokset/2014/en20140917.pdf

Latvia

The Electronic Communications Law, Section 97-101 :
Elektronisko sakaru likums (likumi.lv)

Lithuania

Law on electronic communications of the Republic of Lithuania:
https://www.e-tar.lt/portal/lt/legalAct/TAR.82D8168D3049/asr

Norway

A new legal requirement has been passed. From the 1st of January 2023 onwards Telia Norway has to retain the identity behind IP addresses for 12 months and disclose such data to the police on request. Please see section 2-8 a: https://lovdata.no/dokument/NL/lov/2003-07-04-83#KAPITTEL_2.

Sweden

Electronic Communications Act, Chapter 9, §§ 19-26:
Lag (2022:482) om elektronisk kommunikation Svensk författningssamling 2022:2022:482 t.o.m. SFS 2022:1086 - Riksdagen
Electronic Communications Decree Chapter 9 §§ 4-11:
Förordning (2022:511) om elektronisk kommunikation Svensk författningssamling 2022:2022:511 t.o.m. SFS 2022:1087 - Riksdagen

6. MEASURES TO ADDRES THE DISSEMINATION OF TERRORIST CONTENT ONLINE

To help mitigate the terrorist threat, the EU has adopted the Regulation to address the dissemination of terrorist content online (thereinafter referred to as – TCOR) which applies as of 7th of June 2022. TCOR provides a legal framework to ensure that hosting service providers, that make content available to the public, address the misuse of their services for the dissemination of terrorist content online.

Terrorist content may, according to the TCOR, be any kind of material (including text, images, sound and video recordings, live transmissions) which solicits someone to commit or to contribute to terrorist offences. However, content disseminated for educational, journalistic, artistic or research purposes is exempted. The exemption also applies to content disseminated to raise awareness against terrorist activity.

Telia, being a hosting service provider, is obliged to remove or to disable access to terrorist content within one hour upon receiving a removal order from Member States' competent authorities. EU public register of appointed national competent authorities and contact points is available on EU official website.

Removal orders must contain justifications as to why the material is considered terrorist content, including detailed information on how to challenge the removal order. If needed, Telia may use the right to request a review of the removal order before the relevant authorities. Where content is removed, the user will be informed and provided with information to contest the removal. TCOR provides complaint mechanism to ensure that content that has been removed erroneously can be reinstated as soon as possible.

Following TCOR, Telia shall take proactive measures in case if it is exposed to terrorist content. The measures are to be applied with effective safeguards to protect fundamental rights, in particular freedom of speech. Telia will include in this annual transparency report the measures taken in relation to the identification and removal or disabling access to terrorist content; measures to address the reappearance of terrorist content material, the number of removed or disabled access items following removal orders and the number of removal orders; the number and the outcome of complaints handled; the number and the outcome of administrative or judicial review proceedings brought by Telia; the number of cases in which Telia was required to reinstate content or access thereto as a result of administrative or judicial review proceedings; the number of cases in which Telia reinstated content or access following a complaint by the content provider, etc.

Moreover, Telia's general terms and conditions for hosting services available in its markets, including Sweden, Finland, Estonia, and Lithuania, may further detail its policy for addressing the dissemination of terrorist content, including explanation of specific measures, where applicable.

Telia has not yet (until December 31st, 2022) received removal orders based on the TCOR in any of our markets.

7. GOVERNMENTS' OWN LAW ENFORCEMENT DISCLOSURE REPORTS

We encourage governments to be transparent about their use and scope of surveillance of communications and welcome when they regularly and publicly report to their respective Parliament about the scope of surveillance. Although these publications might not always cover all types of requests and demands, we see government reports as the preferred starting point for discussing best practices. The same governments that adopt surveillance laws should make all reasonable efforts to ensure concerned citizens that these powers are used by the state with due care.

Law Enforcement Disclosure Reports from governments exist in five of our markets:

Denmark

Statistics only published until 2020 by the Prosecution Service: https://anklagemyndigheden.dk/da/statistik

Finland

http://intermin.fi/kertomukset-ja-selvitykset
and
Tiedusteluvalvontavaltuutetun kertomus vuodelta 2021

Lithuania

Telia in Lithuania have not been granted permission to publish our own statistics regarding how many lawful intercept requests we have received. We welcome, however, that Lithuania, like many of the other countries, publishes its own statistics in reports from the State Security Department of Lithuania (SSD). The data is grouped together with other activities, such as access to homes. The latest report for 2021 (page 4) states: "In 2021 SSD has performed actions sanctioned by the district courts against 1,813 individuals. The court sanctioned actions were carried out in respect of 711 citizens of the Republic of Lithuania, 1,061 in relation to foreign citizens and 41 in relation to legal persons."
chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.vsd.lt/wp-content/uploads/2022/05/VSD_Ataskaita4.13.pdf

Norway

https://www.kk-utvalget.no/rapporter.473489.no.html
and additional reporting: https://eos-utvalget.no/eos-utvalgets-arsmelding-for-2021/

Sweden

Redovisning av användningen av hemliga tvångsmedel under 2021, skr. 2022/23:30 (regeringen.se)

https://www.regeringen.se/rattsliga-dokument/skrivelse/2022/12/skr.-20222330/
and additional reporting:
redovisning-av-anvandningen-av-vissa-hemliga-tvangsmedel-under-2021.pdf (aklagare.se)The Swedish Code of Judicial Procedure, 27:16 and 27:16a ('Föreläggande att bevara lagrade uppgifter för brottsutredning') https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/rattegangsbalk-1942740_sfs-1942-740

8. ADDITIONAL TRANSPARENCY MEASURES BY TELIA

The Global Network Initiative (GNI) Country Legal Frameworks Resource

The Global Network Initiative (GNI), in which Telia is an active member, provides a database covering, so far, over 50 countries describing some of the most important surveillance powers available to government agencies and authorities seeking access to customer communications. The work includes reports on three out of Telia's core markets (Denmark, Norway and Sweden). Telia has contributed to the work and will continue to help build this joint resource. The database is available at https://globalnetworkinitiative.org/policy-issues/legal-frameworks/

Telia's tool for assessing and escalating unconventional authority requests is made public

Since the adoption of its freedom of expression policy, Telia has elaborated and updated its internal tool for assessing and escalating governments' requests.

We decided to make the tool publicly available to globally support implementation and further development of industry best practices. We also wanted to open up our tool for rightsholder representatives and other stakeholders to comment on our approach to help build the best possible process together.

The latest version of Telia'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.

Authority requests to block content

We publish statistics using the following blocking categories; Requests from a Government, Authority, or Court to block; DNS, IP-number, URL, and/or VPN. For each of these categories we collect statistics on the number of requests, and the total number of DNSs, IP-numbers, URLs or VPNs requested to be blocked.

This reporting on the extent of authority blocking requests does not cover information on Telia's voluntary commitment to block child sexual abuse material based on a list from either Interpol and/or local law enforcement.

For 2022 we logged that we have been requested to block a total of 1,031 DNS's, 7 IP-numbers, and 11 URLs. A large part of the increased amount of blocking of DNS is the EU sanctions of Russian originated sites.[1]

- Denmark[2]; 7 Requests[3] to block in total 208 DNS
- Estonia; 9 request to block in total 120 DNS
- Finland; 5 requests to block 45 DNS and 2 requests to block in total 11 URLs
- Lithuania; 86 requests to block in total 536 DNS and 5 requests to block in total 7 IP-numbers
- Norway: 1 request to block 4 DNS; and
- Sweden: 9[4] requests to block in total 118 DNS

For 2021 we logged that we have been requested to block a total of 589 DNS's and 5 IP-numbers;

- Denmark[5]; Requests[6] to block in total 8 DNS
- Estonia; 1 request to block in total 85 DNS
- Finland; 0 requests to block
- Lithuania; 38 requests to block in total 253 DNS and 5 requests to block in total 5 IP-numbers
- Norway: 0 requests to block; and
- Sweden: 0[7] request to block in total 240 DNS

[1] The statistics for 2022 include blocking of Russian originated content based on EU sanctions. More information here.
[2] In Denmark, blocking in the area of copyright is not included. Such blockings are made according to a voluntary industry code of conduct when a court has made a decision on blocking and for transparency the industry publishes all copyright related blockings on the following web-page: http://www.tele-indu.dk/brancheholdninger/blokeringer-pa-nettet/
[3] In Denmark blocking of terror sites is set up so that the government provides operators access to a database informing which DNSs to be blocked based on court orders. Such are not included in these statistics.
[4] In Sweden a court-ruling from June 2020 granted rightsholders the right to send lists of DNSs to Telia Sweden for blocking. Rightsholders during 2021 sent a total of 17 lists to Telia Sweden, with a total of 240 sites.
[5] See Note 2
[6] See Note 3
[7] See Note4

For 2020 we logged that we have been requested to block a total of 603 DNS's;

- Denmark[8]; Requests[9] to block in total 49 DNS
- Estonia; 0 requests to block
- Finland; 0 requests to block
- Lithuania[10]; 80 requests to block in total 402 DNS
- Norway[11]: 0 requests to block; and
- Sweden: 1 request to block in total 152 DNS

For 2019 we logged a total of 13 requests to block a total of 518 DNS's;[12]

- Denmark[13]: 9 requests to block in total 82 DNS;
- Estonia: 2 requests to block in total 69 DNS;
- Finland: 0 requests to block;
- Lithuania: Requests to block 210 DNS;
- Moldova: 0 requests to block; and
- Sweden: 2 requests to block in total 157 DNS

[8] See footnote 1
[9] The number of requests was not logged, only the number of DNS's requested to be blocked
[10] Figures corrected in relation to 2020 published report
[11] In Norway, the acquired company GET is included in the calculations from July 2020 and onwards
[12] In Norway, Telia acquired the operator GET in 2018. Work to integrate GET in the statistics was not yet completed in 2019.
[13] See footnote 1

APPENDIX 1. EXTRACT FROM ANNUAL & SUSTAINABILITY REPORT 2022 *– SUBJECT TO LIMITED ASSURANCE*

This extract from the Annual and Sustainability Report 2022 has been subject to limited assurance.

Below from pages 94-95 in the report

Our approach

As a telco and TV and Media provider, Telia's networks and services provide access to information and contribute to the exchange of ideas in a way that supports freedom of expression, openness, transparency, and democracy. At the same time, policymakers increasingly introduce new surveillance measures to fight crime, terrorism, hate speech and more. These measures can potentially limit the freedom of expression and privacy of users and the trust in the services we provide.

Telia is committed to respecting the freedom of expression and right to privacy of users while meeting legal requirements in the countries where we operate. We have clear policy commitments in place and have shaped implementation processes based on input from the Global Network Initiative (GNI), a multi-stakeholder organization that brings together ICT companies, human rights and freedom of press groups, academics, and investors to protect and advance global free expression and privacy in the broadening ICT industry sector.

States define the scope of surveillance and limitations to the free flow of information based on legislation and requests from authorities. We abide by legislation but challenge requests that have no or unclear legal grounds. When there is a conflict between internationally recognized human rights and local legislation, we seek ways to raise the issue with relevant authorities or inform consumers and other stakeholders about the issue through public communications.

Our work is governed by the Group policy – Freedom of expression and surveillance privacy

Our processes

In our work we differentiate between two types of requests from governments/authorities:

• *Conventional requests* are day-to-day requests that are typically of lower risk, such as daily secret real-time wiretapping and monitoring by the police based on court orders. Such requests are received and handled by dedicated local teams.

• *Unconventional requests* are requests that may have serious impacts on users' freedom of expression and privacy. Examples include demands to shut down Internet access, blocking of websites or requirements to retain data for surveillance when legislation is unclear.

Our Group policy and related instruction sets out practical steps regarding assessments and escalation to be performed for unconventional requests. Such requests are to be assessed by the local company and escalated to group level for final joint decisions on how to mitigate human rights risks. While our process aims to identify and mitigate potential violations of individuals' rights, the actual outcome significantly depends on local legislation.

Work during the year

Unconventional requests during the year

During 2022, we closed some 15 unconventional requests and demands across our markets. To ensure consistency, group-level experts facilitated local assessments and escalations. Requests included mainly blocking of specific content on the Internet and removal of TV-stations from Telia TV services, but also new legislation on take-down of terrorist content online, use of anonymized and aggregated data to fight corona, and blocking of mobile calls around prisons. In almost all the cases, Telia took measures to promote freedom of expression and surveillance privacy or mitigate risks in some way, for example by transparency, asking authorities to clarify their requests and/or by being transparent to the public about the request, and always to apply the rule of law. Such actions were defined jointly by local companies and representatives of Telia's Group Executive Management. For information on requests to block Russian originated content, ongoing at the end of the year, please visit our website.

Promoting transparency

When we provide transparency regarding governments' surveillance and actions to limit freedom of expression, we contribute to the protection of users' rights. Making such information more easily accessible has the potential to inform groups whose rights are at risk, including civil society groups working to protect these rights. We therefore publish Law Enforcement Disclosure Reports (LEDR) that include detailed statistics on conventional

requests, as well as the approximate number of unconventional requests. The reports also refer to some of the most relevant legislation. A main element in our reporting on countries' local laws is carried out through contributions to the GNI database on Country Legal Frameworks Resource. Further information about the 2022 LEDR report and the latest statistics are available in Sustainability note S8.

Participation in the Global Network Initiative

To understand our impacts and successfully mitigate risks, we depend on input from stakeholders and experts within this field. Therefore, Telia is an active member of the Global Network Initiative (GNI), which aims to share learnings and leverage when governments act in ways that risk violating freedom of expression and privacy. Telia is a member of the board and participates in various committees and task forces. More information about the work in 2022 is available on the GNI website.

GNI independent assessment of our work

As part of our membership, we have committed to implementing the GNI principles by putting concrete measures in place to promote and advance freedom of expression and the right to privacy. All GNI companies undergo independent assessments of their implementation every two to three years. Results of these assessments are shared with the GNI's multi-stakeholder board, which makes a final determination of the member companies' progress in implementing the GNI principles over time. Telia's second assessment was conducted in 2021/2022. Based on the recommendations in these assessments, Telia has taken the following actions, amongst others:

• Included freedom of expression and surveillance privacy in the company Enterprise Risk Management setup
• Set up a training on human rights for all employees and provided targeted training sessions for the most relevant teams
• Initiated work to review how Telia's due diligence efforts can cover third parties other than suppliers

Based on the assessor's report in May 2022, the GNI Board determined that Telia is making good faith efforts to implement the GNI Principles with improvement over time. More information about the assessment can be found on GNI's website. The GNI will issue a public report in 2023.

Below from pages 120-121 in the report (Sustainability Notes S8 Freedom of expression and surveillance privacy):

In our Law Enforcement Disclosure Reports (LEDR), we publish detailed statistics on conventional requests as well as the approximate number of unconventional requests. The March 2023 LEDR report includes statistics regarding conventional requests from 2020 to 2022. A summary of the findings is presented below as part of the external assurance.

Figures both below and in the LEDR show the number of day-to-day conventional requests from authorities, not the number of individuals to whom they relate. Comparisons between markets should be avoided due to differences in market shares as well as working methods of both authorities and Telia locally. For more information about definitions, data sources and main challenges, see Appendix 2 in the LEDR. For statistics before 2020, please see our resource page for Law Enforcement Disclosure Reports.

Authority requests

NB: Direct access is not included in the statistics.

Denmark

	2022	2021	2020
Lawful interception	4,676	4,310	5,871
Historical data	1,442	1,745	1,947
Subscription data	10,275	7,386	8,924
Challenged / rejected requests	21	0	0

Estonia

	2022	2021	2020
Lawful interception[1]	No statistics	No statistics	Direct access – no statistics
Historical data	7,974	8,835	19,269
Subscription data[2]	670,909	695,335	1,078,670
Challenged / rejected requests	13	20	24

(1) Telia Estonia is not able to provide statistical information to the number of Lawful Interception requests because intercepted numbers as well as the log of requests are encrypted as mandated by the Electronic Communication Act.
(2) The category 'Subscription data' 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.

Finland

	2022	2021	2020
Lawful interception[1]	8,178	6,414	5,218
Historical data	4,982	4,885	3,230
Subscription data	11,109	10.023	10,647
Challenged / rejected requests[2]	75	64	88

(1) In Telia Finland the internal system for logging of lawful intercept requests has been changed. Until March 2021 one individual Lawful interception request was registered as one request, even if it included many types of surveillance measures upon a person. With the system change, the number of requests counted include all surveillance measures. This leads to an increased number in the statistics.
(2) Note that 'Challenged / rejected requests' are in most cases related to erroneous target information from the Police.

Lithuania[1]

	2022	2021
Lawful interception[2]	No permission to publish	No permission to publish
Historical data	97,926	110,138
Subscription data	78,262	96,638
Challenged / rejected requests	24	34

(1) Telia Company and Telia Lithuania had not, until the first half of 2020, been granted permission to publish statistics as to any of the categories regarding how many requests we had received in Lithuania.
(2) Telia Company and Telia Lithuania have not been granted permission to compile and publish our own statistics regarding how many requests we have received in Lithuania for the category Lawful interception. See page 10 for further information.

Norway

	2022	2021	2020
Lawful interception	953	1,067	1,603
Historical data	4,638	4,331 [1]	4,406
Subscription data	9,796	9,419	9,496
Challenged/ rejected requests[2]	71	14	31

(1) Telia Norway from the second half of 2021 and onwards includes manual emergency positioning requests, in accordance with the applicable definition of 'Historical data'. Numbers might therefore be slightly higher than before.
(2) As to the 'Challenged/rejected requests' category, these are invalid requests due to administrative form errors.

Sweden

	2022	2021	2020
Lawful interception	3,729	3,258	3,695
Historical data	7,308	7,142	7,137
Subscription data	3,481	3,074	2,599
Challenged/ rejected requests	197	190	212

APPENDIX 2. – ADDITIONAL INFORMATION REGARDING CONVENTIONAL REQUESTS

Definitions

By *'Lawful interception'* in the above statistics, Chapter 3, we mean secret real-time wiretapping and monitoring by the police and secret police, e.g. real-time access to the content of communications or traffic data ("listening in", wiretapping, 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 in 'Historical data'.

By *'Historical data'* in the above statistics, Chapter 3, 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'* in the above statistics, Chapter 3, we mean numbers (including 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' in the above statistics, Chapter 3, 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 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.

Coverage of our statistics

We report statistics also in markets where governments themselves report and seek to move beyond numbers, complementing quantitative transparency with context for the requests. Throughout the report we aim to demonstrate evidence of how we are embedding our freedom of expression and privacy commitments into our operations. The content of this report also forms the basis for the work we do to advocate for laws and regulations that support the freedom of expression and privacy of our customers and users.

We publish our own statistics covering requests from the police and other authorities in Denmark, Estonia, Finland, Lithuania, Norway and Sweden. 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 for surveillance purposes. Normally, a request is counted into our statistics as soon as a government request has been registered in our respective case management system. The statistics include figures as to the following local authorities:

- Denmark: Danish police and Police intelligence Service.
- Estonia: Police and Border Guard Board ('Politsei- ja Piirivalveamet'), Internal Security Service ('Kaitsepolitseiamet'), Tax and Customs Board ('Maksu- ja Tolliamet'), Ministry of Justice ('Justiitsministeerium') and Foreign Intelligence Service ('Välisluureamet').
- Finland: Police, Finnish Security and Intelligence Service, and Finnish Border Guard. In addition, figures regarding tax authorities are included, since in Finland the police investigate economic crimes in cooperation with the tax authorities.
- Lithuania: State Security Department of Lithuania, Lithuanian Central Bank, Gaming Council Authority, JSC Lithuanian Radio and Television Centre, State Consumer Rights Protection Service.
- Norway: Police ('Politiet'), Criminal Investigation Service ('Politiets sikkerhetstjeneste'), National Criminal Investigation Service ('KRIPOS'), the Police Security Service ('PST') and Rescue/Emergency Services ('HRS').
- Sweden: Police (which in turn include requests from the Secret service), Tax agency (Swedish: 'Skatteverket'), Customs, the Enforcement Authority (Swedish:

'Kronofogdemyndigheten'), and the Economic Crime Authority (Swedish: 'Ekobrottsmyndigheten').

The statistics include figures from companies in our group where Telia has operational control[14] and owns the networks and process for law enforcement disclosure. This means that our figures (except for the category 'Lawful interception') do not cover any requests directed to external service operations because these might be directly responsible for, for example, subscriber information requests.

Main challenges

- Governments have direct access, real-time network access without requests, i.e. 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 has no insight or control 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, (see section 4.).

- Telia's internal systems for interaction with the authorities have normally been set up to handle each single interaction. This means that a request to extend or to discontinue ongoing interception is normally counted as one request in the statistics.

[14] Telia Company does not have full operational control of operations in Latvia, therefore statistics is not included.

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