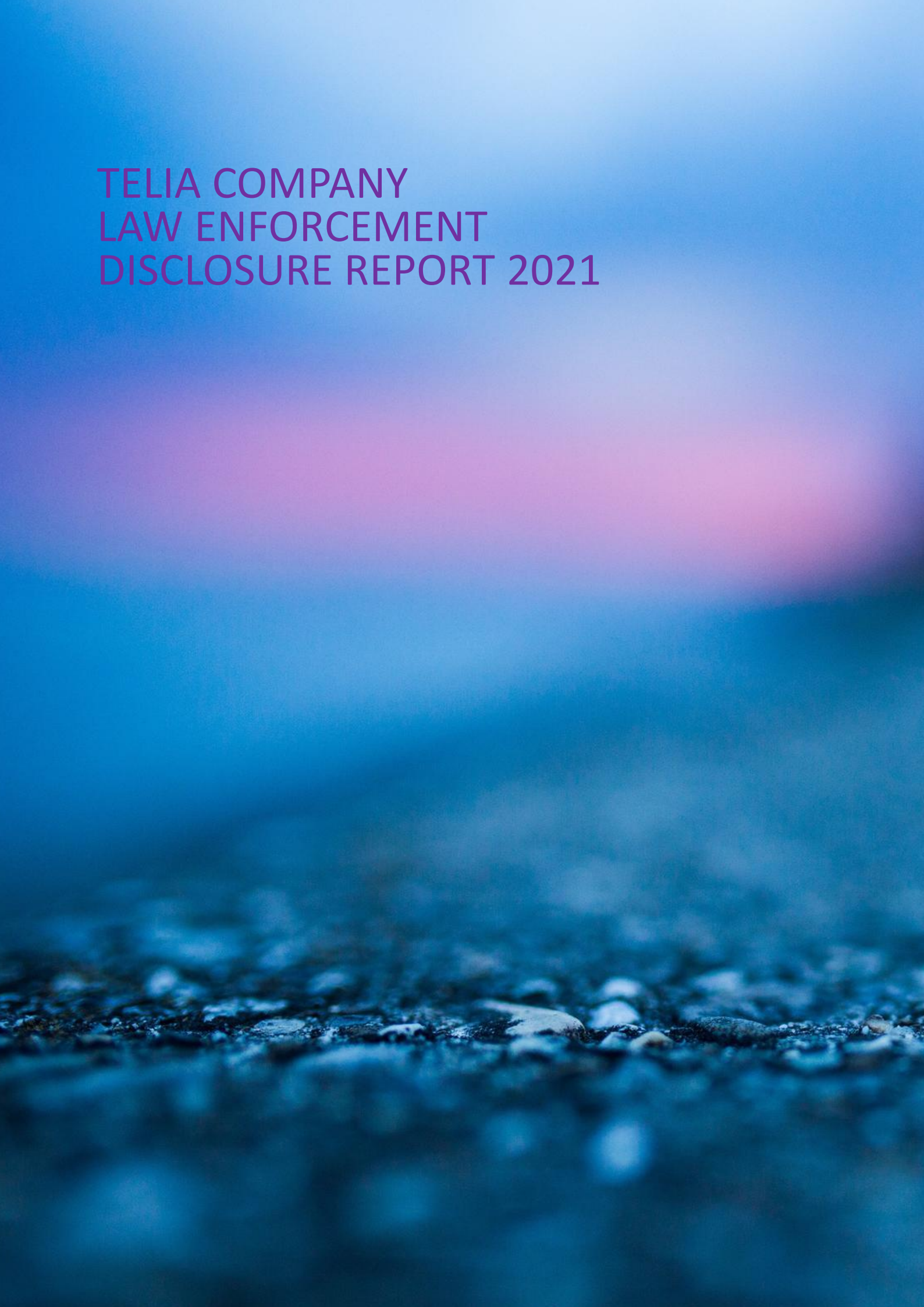
TELIA COMPANY LAW ENFORCEMENT DISCLOSURE REPORT 2021



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 government and authorities in Telia Company's main markets. The report includes statistics on 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 Company labels "major events".

A summarized version of this report is published in the Telia Company 2021 Annual and Sustainability Report available at annualreports.teliacompany.com. This full report provides more context, as well as information about definitions, challenges and the scope of the reporting.

LETTER FROM THE GENERAL COUNSEL AND THE CHIEF EXTERNAL AFFAIRS, GOVERNANCE AND TRUST OFFICER

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 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.

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

According to our policies and procedures, Telia Company 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 privacy are handled in a robust way. However, it is important to stress that the actual outcome of information requests heavily depends on local laws. Governments may also have direct access, where Telia Company 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.

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 publicly shared government reports as the preferred starting point for meaningful transparency, based on the fact that a government can cover not only Telia Company but all operators in any respective country, and also respond to any questions as to the actual necessity and proportionality of the surveillance 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 2021, major events related to such as proposals for new legislation, blocking of content or services, mass surveillance, and requests for voluntary measures. Additional information about those requests can also be found on our website.

Solna March 11th, 2022

Carl Knudsen
Acting Group General Counsel

Rachel Samrén
Senior Vice President, Chief External Affairs, Governance and Trust Officer

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 Company 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 Law Enforcement Disclosure Reporting, our transparency reporting in the context of surveillance, we aim to build user trust and gain the confidence of investors and other stakeholders by demonstrating that Telia Company 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 surveillance powers.

Inevitably, Telia Company makes own judgments 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 2021 have undergone limited assurance as part of the Annual & Sustainability Report assurance process. See Appendix 1 for the information included in the Annual & Sustainability report.

What we report

We have published Law Enforcement Disclosure Reports since 2014. Through this our transparency reporting in the context of surveillance, we aim to build user trust and gain the confidence of investors and other stakeholders by demonstrating that Telia Company 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 surveillance powers.

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 as well as links to laws on mandatory data retention for surveillance.

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)

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 Company Law Enforcement Disclosure Reporting on statistics. See section 3. Starting March 2019, we also started collecting and reporting on the extent of blocking requests, see section 7.

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 sections 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 Category 4.

Reporting on Category 4: Telia Company 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 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 Company'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, such as requests from competition authorities, from 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

Also, 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 Company's commitments as 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.

Telia Carrier operations

In 2020 Telia Company divested Telia Carrier to Polhem Infra. The divestment was closed June 1st, 2021. As to markets in the Nordics and Baltics, any requests to Telia Carrier from January 1st to June 1st were forwarded to the local Telia Company operations.

Telia Carrier's markets outside the Nordics and Baltics are not included in the below reporting on national legislations.

Requests or demands from private entities

Telia Company'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 Company, 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 Company 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 Company'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 requests in the context of freedom of expression and privacy which are not based on law, initiatives for new law-making and significant imposed or proposed operational changes which might potentially have serious impacts on freedom of expression and privacy as 'major events'. 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 that sometimes lack full clarity determine 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 is 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 Company'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 for informed 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 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 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 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 or 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.

Unconventional requests and demands from 2013 to 2019

Please see our earlier reports, available here.

3. STATISTICS FOR CONVENTIONAL REQUESTS

Figures below show the number of day-to-day conventional requests from authorities, not the number of individuals to whom they relate.

Several factors make it difficult to compare statistics between countries. To facilitate comparison over time, previous year's figures have been included. Telia Company has different market shares in different countries, which likely is reflected in the figures. Telia Company 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 some discrepancy of completeness and accuracy 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 Company 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 naturally higher.

Comparisons between markets should be avoided due to differences as to market shares as well as working methods of both authorities and Telia Company locally. For more information about definitions, data sources and main challenges, see Appendix 2.

For statistics before 2019, please see our page for Law Enforcement Disclosure reports here.

Authority requests 2019, 2020 and 2021

NB: As explained earlier, direct access is not included in the statistics. For the overall categorization of government requests, and how we report on these, see in Chapter 1. The below specific categories are defined in Appendix 2.

Denmark

Definitions Appendix 2	H2 2021	H1 2021	H2 2020	H1 2020	H2 2019	H1 2019
Lawful interception	1,980	2,330	2,236	3,635	3,723	4,734
Historical data	871	874	902	1,045	925	1,304
Subscription data	3,545	3,841	3,643	5,281	6,077	6,818
Challenged/ rejected requests	0	0	0	0	0	0

Estonia

Definitions Appendix 2	H2 2021	H1 2021	H2 2020	H1 2020	H2 2019	H1 2019
Lawful interception (1)	No stats. available	No stats. available	No stats. available	No stats. available	No stats. available	No stats. available
Historical data	3,236	5,599	9,377	9,892	9,051	7,776
Subscription data (2)	264,191	431,144	569,137	509,533	447,699	403,602
Challenged/ rejected requests	8	12	11	13	5	14

(1) Telia Estonia is not able to provide statistical information to the number of Lawful Interception requests due to that 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

Definitions Appendix 2	H2 2021	H1 2021	H2 2020	H1 2020	H2 2019	H1 2019
Lawful interception (1)	2,953	3,461	2,700	2,518	2,177	2,590
Historical data	2,506	2,379	1,552	1,678	1,623	1,328
Subscription data	4,920	5,103	5,480	5,167	4,627	6,323
Challenged/ rejected requests (2)	27	37	45	43	43	28

(1) In Finland the 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 cases are in most cases related to erroneous target information from the Police.

Lithuania (1)

Definitions Appendix 2	H2 2021	H1 2021	H2 2020
Lawful interception (2)	No permission to publish	No permission to publish	No permission to publish
Historical data	59,719	50,419	43,649
Subscription data	51,695	44,943	55,780
Challenged/ rejected requests	10	24	22

(1) Telia Company and Telia Lithuania had not, until H2 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 for the category Lawful interception we have received in Lithuania. See page 10 for further information.

Norway (1)

Definitions Appendix 2	H2 2021	H1 2021	H2 2020	H1 2020	H2 2019	H1 2019
Lawful interception	560	507	726	877	1,239	572
Historical data	5,606 (2)	3,838	3,227	3,055	5,051	2,444
Subscription data	4,363	5,056	4,349	5,147	10,426	5,066
Challenged/ rejected requests (3)	1	13	17	14	37	20

(1) Telia Norway acquired the operator Get in 2018. Get is integrated into the statistics since July 2020.

(2) Telia Norway from H2 / 2021 onwards includes manual emergency positioning requests, in accordance with the applicable definition of 'Historical data'. Numbers might therefore be slightly higher than before.

(3) As to the category 'Challenged/rejected requests', these are invalid requests due to administrative form errors.

Sweden

Definitions Appendix 2	H2 2021	H1 2021	H2 2020	H1 2020	H2 2019	H1 2019
Lawful interception	1,217	2,041	1,704	1,991	1,738	1,920
Historical data	3,876	3,266	3,462	3,675	2,679	2,629
Subscription data	1,625	1,449	1,364	1,235	900	836
Challenged/ rejected requests	84	106	107	105	185	176

4. LAWS PROVIDING GOVERNMENTS' DIRECT ACCESS

The United Nations, in its Resolution on the 'Promotion, protection and enjoyment of human rights on the Internet' from June 2016: (link here)

"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.* "

When it comes to governments' direct access, i.e. 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 Company 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 geographies 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 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 and surveillance privacy is at stake. Telia Company'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 with 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 2022) 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: (http://likumi.lv/doc.php?id=96611), Section 69 "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/ZpNMZQSaRN
Code of Criminal Procedure of the Republic of Lithuania:
https://www.e-tar.lt/portal/lt/legalActEditions/TAR.EC588C321777
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

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 Company 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

Executive Order No. 988 28/9-2006 with amendments on providers of electronic communications networks and services' registration and storage of information about telecommunications traffic (data retention):
https://www.retsinformation.dk/Forms/R0710.aspx?id=2445

New data retention rules are being heard by Parliament. The proceeding can be followed here: https://www.ft.dk/samling/20211/lovforslag/l93/index.htm

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 71.1 "Utilization and Processing of Data to be Retained":
https://likumi.lv/ta/id/96611

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

Norway

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.

Sweden

Electronic Communications Act, Chapter 6, §§ 16a-f:
https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2003389-om-elektronisk-kommunikation_sfs-2003-389
Electronic Communications Decree §§ 37-46:
https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2003396-om-elektronisk_sfs-2003-396

6. 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

https://anklagemyndigheden.dk/sites/default/files/inline-files/Revideret%20udkast%20-%20Statistik%20over%20indgreb%20i%20meddelelseshemmeligheden%20og%20ransagninger%20i%202019%20%28004%29.pdf%201_1.pdf
and additional reporting:
https://anklagemyndigheden.dk/da/statistik

Finland

http://intermin.fi/kertomukset-ja-selvitykset
and
https://tiedusteluvalvonta.fi/-/tiedusteluvalvontavaltuutettu-julkaisi-toisen-vuosikertomuksensa

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 2020 (page 4) states: "In 2020 SSD has performed actions sanctioned by the district courts against 1,775 individuals. The court sanctioned actions were carried out in respect of 773 citizens of the Republic of Lithuania, 946 in relation to foreign citizens and 56 in relation to legal persons."
https://www.vsd.lt/wp-content/uploads/2021/05/Ataskaita_2020_viesa_galutinis-3.pdf

Norway

https://www.kk-utvalget.no/rapporter.473489.no.html
and additional reporting:
https://eos-utvalget.no/wp-content/uploads/2020/03/EOS-a%CC%8Arsmelding-2019-nett.pdf

Sweden

Redovisning av användningen av hemliga tvångsmedel under 2020, skr. 2021/22:79 (regeringen.se)
and additional reporting:
Redovisning av användningen av vissa hemliga tvångsmedel under 2020 (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

7. ADDITIONAL TRANSPARENCY MEASURES

The Global Network Initiative (GNI) Country Legal Frameworks Resource

The Global Network Initiative (GNI), in which Telia Company 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 Company's core markets (Denmark, Norway and Sweden). Telia Company has contributed to this work and will continue to help building this joint resource.

The database is available at https://globalnetworkinitiative.org/policy-issues/legal-frameworks/

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

Since the adoption of its freedom of expression policy, Telia Company 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 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.

Authority requests to block content

In March 2019, Telia Company started to report also on the extent of authority blocking requests. The reporting 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.

We collect statistics using the following blocking categories; Requests from Government, Authority, Court to block;

- DNS;
- IP-number;
- URL; and
- 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 blocked.

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

- Denmark[1]; Requests[2] 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[3] request to block in total 240 DNS

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

- Denmark[4]; Requests[5] to block in total 49 DNS
- Estonia; 0 requests to block
- Finland; 0 requests to block
- Lithuania[6]; 80 requests to block in total 402 DNS
- Norway[7]: 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;[8]

- Denmark[9]: 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.

[1] 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.teleindu.dk/brancheholdninger/blokeringer-pa-nettet/

[2] 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.

[3] 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.

[4] See footnote 1

[5] The number of requests was not logged, only the number of DNS's requested to be blocked

[6] Figures corrected in relation to 2020 published report

[7] In Norway, the acquired company GET is included in the calculations from July 2020 and onwards

[8] In Norway, Telia acquired the operator GET in 2018. Work to integrate GET in the statistics was not yet completed in 2019.

[9] See footnote 1

APPENDIX 1. - EXTRACT FROM ANNUAL & SUSTAINABILITY REPORT 2021

This extract from the Annual and Sustainability Report 2021 has been subject to limited assurance.

Below from pages 97-98

Our approach

The networks and services - provided by us as a telco and a TV and Media provider -give access to information and the exchange of ideas in a way that supports freedom of expression, openness, transparency and democracy. At the same time policymakers introduce new surveillance measures to fight crime, terrorism, hate speech and more. These are measures that can potentially limit the freedom of expression and privacy of users and the trust in what we provide.

Telia Company is committed to respect 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 (see further next page). To ensure transparency and confirm compliance, our work is regularly reviewed through independent assessments.

States define the scope of surveillance and limitations to the free flow of information based on legislation and requests from authorities. We abide by such 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 for 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 differ between two types of requests from governments/authorities:

• Conventional requests are day-to-day requests that are typically of lower risk, such as 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 such which may have serious impacts on the freedom of expression and privacy of users. Examples include demands to shut down internet access, blocking of websites or requirements to retain data for surveillance when legislation is unclear.

Our Group 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 decisions regarding which measures to take to mitigate human rights risks. We adhere to local legislation while also implementing measures that respect and support the rights of individuals. In addition, we aim to publicly share as much information as possible about unconventional requests. While our process is intended to identify and mitigate potential violations of individuals' rights, the actual outcome depends significantly on local legislation.

Work during the year

Unconventional requests during the year

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 or 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.

Promoting transparency

We believe that transparency on governments' surveillance and actions to limit freedom of expression contribute to protecting 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) which include detailed statistics on conventional as well as the approximate number of unconventional requests. The reports also refer to some of the most relevant legislations. 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 2021 LEDR report and the latest statistics are available in Sustainability note S8 (Annual and Sustainability Report 2021, page 116).

Below from page 116 (Sustainability Notes):

We publish detailed statistics on conventional as well as the approximate number of unconventional requests in our Law Enforcement Disclosure Reports (LEDR). The March 2022 LEDR report includes statistics regarding conventional requests from 2019, 2020 and 2021. 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 as to market shares as well as working methods of both authorities and Telia Company locally. For more information about definitions, data sources and main challenges, see Appendix 2 in LEDR. For statistics before 2019, please see our resource page for Law Enforcement Disclosure Reports here.

Authority requests 2019, 2020 and 2021

NB: Direct access is not included in the statistics.

Denmark

	2021	**2020**	**2019**
Lawful interception	4,310	5,871	8,457
Historical data	1,745	1,947	2,229
Subscription data	7,386	8,924	12,895
Challenged / rejected requests	0	0	0

Estonia

	2021	**2020**	**2019**
Lawful interception[1]	No statistics	Direct access – no statistics	Direct access – no statistics
Historical data	8,835	19,269	16,827
Subscription data[2]	695,335	1,078,670	851,301
Challenged / rejected requests	20	24	19

(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

	2021	**2020**	**2019**
Lawful interception[3]	6,414	5,218	4,767
Historical data	4,885	3,230	2,951
Subscription data	10.023	10,647	10,950
Challenged / rejected requests[4]	64	88	71

(3) In Finland the 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.

(4) Note that 'Challenged / rejected requests' are in most cases related to erroneous target information from the Police.

Lithuania[5]

	2021	2020 July - Dec
Lawful interception[6]	No permission to publish	No permission to publish
Historical data	110,138	43,649
Subscription data	96,638	55,780
Challenged / rejected requests	34	22

(5) Telia Company and Telia Lithuania had not, until H2 2020, been granted permission to publish statistics as to any of the categories regarding how many requests we had received in Lithuania.

(6) Telia Company and Telia Lithuania have not been granted permission to compile and publish our own statistics regarding how many requests for the category Lawful interception we have received in Lithuania. See page 10 in the full LEDR report for further information.

Norway[7]

	2021	2020	2019
Lawful interception	1,067	1,603	1,239
Historical data	9,444 [8]	6,282	5,051
Subscription data	9,419	9,496	10,426
Challenged/ rejected requests[9]	14	31	37

(7) Telia Norway acquired the operator Get in 2018. Get is included in the statistics since July 2020.

(8) Telia Norway from H2 / 2021 onwards includes manual emergency positioning requests, in accordance with the applicable definition of 'Historical data'. Numbers might therefore be slightly higher than before.

(9) As to the 'Challenged/rejected requests' category, these are invalid requests due to administrative form errors.

Sweden

	2021	2020	2019
Lawful interception	3,258	3,695	3,658
Historical data	7,142	7,137	5,308
Subscription data	3,074	2,599	1,736
Challenged/ rejected requests	190	212	361

Unconventional requests and demands

Information reported about unconventional requests in the *Freedom of expression and surveillance privacy* section is also externally assured.

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", 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 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 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.

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. Normally, a request is counted into our statistics as soon as a government request has been registered in our respective case management system.

- Denmark: The statistics include figures regarding the Police Intelligence Service.
- Estonia: The statistics include figures regarding the 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: The statistics include the police, secret service, and customs. In addition, figures regarding tax authorities are included, since in Finland the police investigate economic crimes in cooperation with the tax authorities.
- Lithuania: The State Security Department of Lithuania.
- Norway: The statistics include figures regarding the Police ('Politiet'), Criminal Investigation Service ('Politiets sikkerhetstjeneste'), National Criminal Investigation Service ('KRIPOS'), the Police Security service ('PST') and Rescue/Emergency Services ('HRS').
- Sweden: The statistics include figures regarding the 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 Company has operational control[10] and 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, for example, subscriber information requests.

Main challenges

- Governments have direct access, i.e. 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 Company 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 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 ongoing interception is counted as one request in the statistics.

- Regarding the category of lawful interception, the number of requests is most likely larger than the number of individuals concerned.

- In contrast to the previous point however, 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), 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. 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 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 usually and over time receive 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.

[10] 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