TeliaSonera Law Enforcement Disclosure Report
July – December 2015

Content

Executive summary .............................................................................................................. 2
Letter from the General Counsel ......................................................................................... 3
About this report .................................................................................................................. 4
Why we are reporting .......................................................................................................... 4

Law Enforcement Disclosure statistics and context as part of 2015 Annual and Sustainability Report. This text, pages 6-8, has been subject to limited assurance ........................................ 6
Statistics day-to-day requests from Jan 2014 to Dec 2015 .................................................... 9
Definitions ............................................................................................................................ 10

Unconventional requests and demands ............................................................................. 12
A. Unconventional requests and demands 2013 ................................................................. 12
B. Unconventional requests and demands January to June 2014 ...................................... 12
C. Unconventional requests and demands July to December 2014 .................................. 13
D. Unconventional requests and demands January to June 2015 ..................................... 13
E. Unconventional requests and demands July to December 2015 .................................. 13

Laws providing governments direct access ........................................................................ 15
Market ................................................................................................................................. 15
Legislation ........................................................................................................................... 15
Azerbaijan .......................................................................................................................... 15
Denmark ............................................................................................................................. 15
Estonia ................................................................................................................................. 15
Finland ................................................................................................................................. 16
Georgia ............................................................................................................................... 16
Kazakhstan ......................................................................................................................... 16
Latvia ................................................................................................................................. 16
Lithuania ............................................................................................................................... 16
Moldova .............................................................................................................................. 17
Nepal ................................................................................................................................. 17
Norway ............................................................................................................................... 17
Sweden ............................................................................................................................... 17
Tajikistan ............................................................................................................................ 17
Uzbekistan ......................................................................................................................... 17

Reported cases ................................................................................................................... 19
Case on shared learning: Publicly sharing TeliaSonera’s up-dated tool for assessing and escalating unconventional authority requests ...................................................................................... 19

Questions and Answers ................................................................................................... 20
Scope .................................................................................................................................. 22

Main goals, challenges and omissions .............................................................................. 23
Main goals .......................................................................................................................... 23
Main challenges .............................................................................................................. 23
Not included in this here reporting ................................................................................... 23

Further information ......................................................................................................... 24
Report on local laws ......................................................................................................... 24
New version of the TeliaSonera Group Freedom of Expression Policy .............................. 24
Government law enforcement disclosure reports .............................................................. 24

Executive summary

This report aims to provide insights into the extent of authorities’ access to, and collection of, customer data in TeliaSonera’s markets. This is our fourth 6-monthly Law Enforcement Disclosure Report (first two issues named ‘Transparency Report’). The aim is to offer detailed insight into the context and extent of surveillance. It includes statistics of number of requests in nine of our markets as well as information on legislation regarding ‘direct access’ in all of our markets.

A summarized version of this report is published in the TeliaSonera 2015 Annual and Sustainability Report, available here. The full report, below, includes more contexts, including such as additional chapters on ‘Unconventional requests and demands’ as well as a questions and answers section and a chapter on main goals, challenges and omissions.
Letter from the General Counsel

Millions of customers trust TeliaSonera to provide telecommunications services. They trust TeliaSonera to protect their communications, data and personal information. In return we publish Law Enforcement Disclosure Reports to contribute to an open and transparent world where customer privacy and freedom of expression are at the forefront.

Maintaining customer privacy is of utmost importance at TeliaSonera: It is one of the pillars of our Group Code of Ethics and Conduct. At the same time, TeliaSonera 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 are based on specific reasons, such as enforcing criminal law and safeguarding national security. We also provide assistance to emergency services in response to life threatening situations and emergency calls.

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

The issues are complex. Different stakeholders have different views. But 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 international human rights standards allow. Limitations must be necessary and proportionate and clearly delineated within a strong legal framework with the right checks and balances. When there is an opportunity, we argue for legislation to promote human rights.

We encourage governments to be transparent about their use and scope of surveillance of communications. We welcome reports – such as the ones in Denmark, Finland, Norway and Sweden – where each respective government regularly and publicly reports to their Parliament about the scope of their surveillance. Although these publications might not always cover all kinds of requests and demands, we see publicly shared government reports as the preferred starting point for discussing best practice for meaningful transparency, considering that a government can cover all telecom operators in any respective country and also respond to any questions as to proportionality of surveillance.

To supplement government reporting, TeliaSonera wants to make it transparent to our customers and stakeholders to what extent authorities require access to data of our customers and communications. Our aim is to contribute to a meaningful oversight and discussion of the proper limits of government surveillance powers. We will therefore continue to publish Law Enforcement Disclosure Reports regularly every six months.

In this TeliaSonera Transparency Report we continue publishing statistics covering requests from the police and other authorities in Denmark, Estonia, Finland, Georgia, Moldova, Nepal, Norway, Spain and Sweden. We plan to update our reporting twice a year, to coincide with the publishing of our Annual and Sustainability Report (every year in March) and the sustainability update (every October). The table included in this report shows the number of authority requests in each country based on a court order or other legal demand by the police or other authority. Our aim is to add similar statistics from additional TeliaSonera markets to our reporting, aiming for transparency to the greatest extent possible in all our markets in the future.

In addition to the reporting of statistics, this report provides information on unconventional requests or demands from governments, as well as requests and demands with potentially serious impacts on the freedom of expression within the telecommunications industry. In accordance with our Freedom of Expression policy, we identify such exceptional and unconventional requests and demands as ‘major events’.

Stockholm March 22, 2016

Jonas Bengtsson
Senior Vice President and General Counsel
TeliaSonera
About this report

What we publish and what is new information compared to our report October 2015:

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

- Updated statistics as to the nine markets we covered in our report October 2015;
- Elaborated on ‘Unconventional requests and demands’; and
- Discontinued reporting on requests for emergency positioning.

The statistics below on law enforcement disclosure requests include:

- January – December 2013 - Two countries
- January – June 2014 - Two countries
- July – December 2014 - Seven countries
- January – June 2015 - Nine countries
- July – December 2015 – Nine countries - Added in this report

The next report is planned to be published in October 2016.

In this report, we publish statistics covering requests from the police and other authorities in Denmark, Estonia, Finland, Georgia, Moldova, Nepal, Norway, Spain and Sweden. We plan to update our reporting twice a year (bi-annually) to coincide with the publishing of the Annual and Sustainability Report (every March) and the sustainability update (every October).

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.

Our aim is to add similar statistics from additional TeliaSonera markets to our upcoming reports. We therefore continue to analyze the legal situation in other regions and aim for transparency to the greatest extent possible in all our markets in the future. However, it should be noted that there is an on-going challenge in that in some countries where laws governing disclosure might remain unclear. In addition, in certain countries, there might be potential risks for our employees which could arise from our commitment to increase public awareness and transparency. Analyzing legal powers and operating practices of governments within the realm of surveillance can be critically sensitive matters.

At TeliaSonera, requests from law enforcement authorities are handled by specially set-up units that have been trained to handle these requests according to the processes in place.

All requests from authorities must be legally correct. TeliaSonera is to reject or challenge any request that does not conform to the established form and process, for example when a form has not been signed or has not been sent by an appropriate sender. In such cases the process is for TeliaSonera to ask for clarification.

With this report, as of March 2016, we discontinue reporting on requests for emergency positioning, see chapter ‘Main goals, challenges and omissions’ below.

WHY WE ARE REPORTING

This report aims to provide insights into the extent of authorities’ collection of customer data for law enforcement purposes in nine of TeliaSonera’s markets. This is a part of TeliaSonera’s commitment to respect freedom of expression. Operators must adhere to law enforcement requirements which may impact an individual’s privacy and freedom of expression. What TeliaSonera can do is to inform its customers and stakeholders of the extent of use of such surveillance, including within which legal context.

According to our policies and procedures, TeliaSonera discloses information to authorities only to the extent required by law or with the customer’s permission. This is a non-negotiable part of the way we operate. It should be noted that, within this context, governments also have direct access, i.e. signals intelligence and real-time access without having to send requests to the operators.

Regarding such direct access, TeliaSonera has no insight into the extent of surveillance and cannot provide statistics. Therefore, we publish a chart with links to legislation providing the authorities with such direct access in this report.

By publishing law enforcement disclosure statistics, TeliaSonera wants to make it transparent to our customers and stakeholders to what extent authorities require access to data. Our aim is to contribute to a meaningful oversight and discussion regarding the proper limits of government surveillance powers.

Several factors make it difficult to compare the statistics between countries. TeliaSonera has different market shares in different countries, which is probably reflected in the figures. Furthermore, TeliaSonera is not privy to each authorities’ working methods and priorities in different countries, and these methods are likely to differ. Also, within TeliaSonera, there are different working methods in different countries. This causes issues related to completeness and accuracy of reported data. See further the Questions and Answers (Q&A) section in this report titled “Why the figures differ between countries”. We work to streamline these working methods and define best practice, to further improve data quality.
It should also be noted that the figures show the number of requests from authorities, not the number of individuals that have been targeted. Not even TeliaSonera as the operator and provider of the information has this knowledge. Within the category of lawful interception, the number of requests is most likely larger than the number of individuals that have been targeted. As to requests for cell tower dumps (i.e. requests that oblige TeliaSonera to disclose data about the identity, activity and location of any device that connects to targeted cell towers over a set span of time) the number of affected individuals will naturally become larger than the number of requests.

The statistics are presented in the context of surveillance and law enforcement, and therefore do not include requests from authorities that have no role in lawful interception or other services obligated for operators, such as requests from competition authorities and national regulatory authorities.

The statistics include figures from companies in TeliaSonera Group where TeliaSonera owns the networks and process for law enforcement disclosure. Thus, the figures do not cover requests directed to external service operators (such as Fujitsu in Finland) except for the lawful interception category.

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

The categories are explained briefly below the charts and in more detail in the chapter ‘Definitions’ and the subsection, ‘Requests from authorities’.

According to the Freedom Online Coalition¹, there is a need to move beyond figures:

“Transparency reports published by companies and a few governments that have tended to focus on the numbers of requests can be strengthened by providing greater context. This might include explanations of the policies and processes governments and companies follow, illustrative examples of requests, and narrative content describing the data, including how it might differ from previous reports.” (1)

Our aim is for the TeliaSonera Law Enforcement Disclosure Reports to meet this need.

---

¹ Freedom Online Coalition report May 2015, ‘Working group 3, Privacy and Transparency Online’
Law Enforcement Disclosure statistics and context as part of 2015 Annual and Sustainability Report. This text, pages 6-8, has been subject to limited assurance

**FREEDOM OF EXPRESSION AND PRIVACY**

<table>
<thead>
<tr>
<th>STRATEGIC OBJECTIVE</th>
<th>2018 GOALS</th>
<th>2015 OUTCOME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable, respect and support freedom of expression and privacy. We are regarded as the trusted ICT industry leader in human rights.</td>
<td>All markets covered in law enforcement disclosure with regards to statistics on government requests. All markets covered in law enforcement disclosure with regards to information on local legislation. All closed unconventional requests challenged. Actively contribute to the work of the Telecommunications Industry Dialogue and its collaboration with the Global Network Initiative.</td>
<td>0 countries covered in law enforcement disclosure with regards to statistics on government requests. 5 countries covered in law enforcement disclosure with regards to information on local legislation. Just above half of closed unconventional requests challenged. Contributed to the ID and UN joining forces.</td>
</tr>
</tbody>
</table>

Telecommunications enable the exchange of ideas and access to information in a way that supports openness and transparency. It is our duty to respect our customers’ and users’ freedom of expression and privacy.

The right to customer privacy is widely understood as an essential requirement for the right to freedom of expression. Therefore, we have direct commitments both as to surveillance privacy (when authorities require access to user data) and to customer privacy (our processing of customer data for our own needs). See more about our customer privacy work in “Customer privacy.”

**CONTEXT**

Issues related to freedom of expression and privacy pose a high risk to users of telecom services globally. Such risks include mass surveillance, network shutdowns, localization of mobile devices and blocking or restriction of certain content. Through legislation and decisions from authorities, states define the scope of surveillance of communications and limitations to the free flow of information.

ICT and human rights in general, and freedom of expression and privacy in particular, have gained attention through developments in recent years, such as surveillance revelations and terrorist attacks. We foresee that our work will become increasingly important throughout all our markets as legislators seek additional surveillance measures to fight crime and terrorism.

**GOVERNANCE**

Respecting freedom of expression and privacy

By putting processes in place, we aim to fulfill our responsibility and commitments to respect freedom of expression and privacy as laid out in the UN Guiding Principles for Business and Human Rights. Our duty to respect and promote human rights is focused on the risks to our customers. We aim to limit potential harm to individuals by seeking active measures to support the rights of our customers where we believe that those are at risk.

Our freedom of expression and privacy work is guided by the UN Guiding Principles, the Telecommunications Industry Dialogue Principles on Freedom of Expression and Privacy and the group policy on freedom of expression in telecommunications.
The policy addresses our commitments in relation to requests or demands with potentially serious impacts on freedom of expression in telecommunications, such as mass surveillance where authorities demand unrestricted real-time network access, shutdown of all or parts of a network, blocking or restricting access to specific content, blocking or restricting access to services or networks and proposals for new laws or significant operational changes.

We have highlighted the importance of freedom of expression in our CEO's statement, see www.teliasonera.com/en/sustainability/human-rights.

Assessment and escalation
A group instruction sets out practical steps regarding assessments and escalation that are instructed to be carried out whenever a local company receives a request or demand that may have potentially serious impacts on freedom of expression in telecommunications. Guidance is provided in a form for assessments and escalation, a tool that we have shared publicly.

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

ACTIVITIES DURING THE YEAR

Stakeholder engagement
The Industry Dialogue (ID), which in December 2015 included nine international telecom companies, adds leverage to advocacy promoting freedom of expression and privacy in the telecommunications industry. Our active participation stimulates shared learning on how to best respect freedom of expression and privacy. A description of the ID's activities during the year is available at www.telecomindustrydialogue.org. Our work with regard to the ID Principles is available in a document at www.teliasonera.com/sustainability/reports.

The ID has a formal collaboration with the multi-stakeholder Global Network Initiative (GNI). By working together, the two initiatives aim to advance freedom of expression and privacy rights in the ICT sector more effectively. The collaboration provides a common platform for shared learning and leverage. In January 2016, the ID and GNI agreed to combine. We have been active in promoting the collaboration, which will take full effect in 2017.

We have promoted the ID Principles at MegaFon and Turkcell. These dialogues will continue during 2016.

Law enforcement disclosure reporting
We believe that transparency on surveillance activities can contribute to a world where customer privacy and freedom of expression are more strongly enforced. Therefore we publish law enforcement disclosure reports twice a year. In 2015, we published such reports in January and October. The reports can be found at www.teliasonera.com/sustainability/reports.

The most recent report, released alongside this Annual and Sustainability Report, includes statistics covering requests from the police and other authorities in nine countries. The statistics, as presented in the table below, show the number of authority requests in each country based on a court order or other legal demand by the police or other authority. The statistics are subject to limited assurance by Deloitte.

Authority requests* 2016

<table>
<thead>
<tr>
<th>Country</th>
<th>Lawful interception</th>
<th>Historical data</th>
<th>Subscription data</th>
<th>Challenges/rejected requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denmark</td>
<td>3,029</td>
<td>2,488</td>
<td>9,812</td>
<td>35</td>
</tr>
<tr>
<td>Estonia</td>
<td>1,014</td>
<td>2,296</td>
<td>28,037</td>
<td>4,768*</td>
</tr>
<tr>
<td>Finland</td>
<td>4,289</td>
<td>2,078</td>
<td>7,807</td>
<td>20</td>
</tr>
<tr>
<td>Georgia</td>
<td>Not available</td>
<td>284</td>
<td>1,302</td>
<td>816*</td>
</tr>
<tr>
<td>Moldova</td>
<td>Not available</td>
<td>10,245</td>
<td>5,925</td>
<td>330*</td>
</tr>
<tr>
<td>Nauru</td>
<td>Not available</td>
<td>19,905</td>
<td>37,022</td>
<td>0</td>
</tr>
<tr>
<td>Norway</td>
<td>3,295</td>
<td>5,234</td>
<td>9,172</td>
<td>137*</td>
</tr>
<tr>
<td>Spain</td>
<td>20,410</td>
<td>26,079</td>
<td>43,909</td>
<td>770</td>
</tr>
<tr>
<td>Sweden</td>
<td>2,540</td>
<td>1,253</td>
<td>4,017</td>
<td>338</td>
</tr>
</tbody>
</table>

1 As explained in the text, direct access is not included in the statistics.
2 In Estonia, a closed access system is used. We keep a log of these requests.
3 This figure includes all requests for Subscription data. For other countries the corresponding report only access requests that are handled by authorized personnel.
4 This figure indicates all requests to which we were not able to answer, most often because the requested information was about a customer of another operator.

Differences in market share as well as working methods, both by authorities and within TeliaSonera, make it difficult to compare statistics between countries. For definitions of the categories, see the Law Enforcement Disclosure Report at www.teliasonera.com/sustainability/reports.

Our reporting of country legal frameworks pertaining to freedom of expression and privacy in telecommunications is performed through contribution to the ID database on country legal frameworks. Our law enforcement disclosure report includes links to national laws that provide governments with direct access to information about our customers and their communication, without having to request information from TeliaSonera.

Regarding governments' direct access, i.e. signals intelligence (intelligence gathering through analysis and processing of communication signals) and real-time access without requests (technical systems for more extensive monitoring of telecommunications), TeliaSonera has no insight into the extent of such surveillance (when, who and what) and cannot provide any statistics beyond those provided within this report.
Unconventional requests
In addition to reporting statistics, we publish information on unconventional requests or demands from governments ("major events"). During 2015, we closed some 15 such unconventional requests or demands from governments across our operations. To support the decision making process and ensure a consistent view on freedom of expression throughout the group, we facilitated local company risk assessments and escalations. Points of challenge, where possible, were defined jointly by local, regional and group management.

Main challenges to reporting
We seek to be as transparent as possible, but there are challenges. Local laws that may sometimes look full clarity determine what we can and cannot publish. As to unconventional requests, there may be either confidentiality provisions or constraints based on our duty to protect the safety of our personnel. Also, issues regarding direct access are closely related to national security and therefore challenging to share and communicate.

Counting the number of unconventional requests is difficult and subjective as such requests can range from a demand to block one or several websites, shutting down of a network locally to requests regarding direct access.

PLANNED ACTIVITIES IN 2016
We will continue our work regarding law enforcement disclosure reporting. We aim to find ways to standardize such reporting within the ID and SNI.

TeliaSonera will continue to respect and promote human rights in general. This includes further elaboration of assessment processes, training, compliance monitoring and review. The aim is for this work to benefit from the shared learning and leverage within the context of the ID and SNI. Specific gaps in our work include:
- Shared learning and implementation in ramadgy and grievance mechanisms.
- Local stakeholder dialog and engagement.
- Governance and training to make the process of assessments and escalations swift, especially when it comes to requests and demands for direct access to our networks and systems.

CASE:
INFORMATION ON UNCONVENTIONAL REQUESTS
TeliaSonera aims to publish information about every unconventional request or demand from governments ("major events"). Below is a list of articles from July through December 2015 on such major events. A list of major events in January through June 2015 can be found in the Sustainability Update at www.teliasonera.com/sustainability.


# TeliaSonera Law Enforcement Disclosure Report
## July – December 2015

## Statistics day-to-day requests from Jan 2014 to Dec 2015

### Authority requests*
**July 1 – December 31 2015**

<table>
<thead>
<tr>
<th>Country</th>
<th>Lawful interception</th>
<th>Historical data</th>
<th>Subscription Data</th>
<th>Challenged/rejected requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denmark</td>
<td>3000</td>
<td>661</td>
<td>4687</td>
<td>27</td>
</tr>
<tr>
<td>Estonia</td>
<td>1704 *1</td>
<td>990</td>
<td>133,687 *2</td>
<td>1619 *3</td>
</tr>
<tr>
<td>Finland</td>
<td>2207</td>
<td>1129</td>
<td>4312</td>
<td>14</td>
</tr>
<tr>
<td>Georgia</td>
<td>Not available *4</td>
<td>90</td>
<td>560</td>
<td>241</td>
</tr>
<tr>
<td>Moldova</td>
<td>Not available *4</td>
<td>5261</td>
<td>2816</td>
<td>101</td>
</tr>
<tr>
<td>Nepal</td>
<td>Not available *4</td>
<td>18220</td>
<td>20519</td>
<td>0</td>
</tr>
<tr>
<td>Norway</td>
<td>988</td>
<td>3002</td>
<td>4762</td>
<td>83</td>
</tr>
<tr>
<td>Spain</td>
<td>10183</td>
<td>16177</td>
<td>20112</td>
<td>339</td>
</tr>
<tr>
<td>Sweden</td>
<td>1555</td>
<td>1062</td>
<td>1711</td>
<td>74</td>
</tr>
</tbody>
</table>

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

### Authority requests*
**January 1 – June 30 2015**

<table>
<thead>
<tr>
<th>Country</th>
<th>Lawful interception</th>
<th>Historical data</th>
<th>Emergency positioning</th>
<th>Subscription data</th>
<th>Challenged/rejected requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denmark</td>
<td>2,825</td>
<td>707</td>
<td>145,305</td>
<td>4,985</td>
<td>11</td>
</tr>
<tr>
<td>Estonia</td>
<td>1,750 *1</td>
<td>1,236</td>
<td>900,390</td>
<td>154,736 *2</td>
<td>3,129 *3</td>
</tr>
<tr>
<td>Finland</td>
<td>2,187</td>
<td>949</td>
<td>422,260</td>
<td>3,555</td>
<td>12</td>
</tr>
<tr>
<td>Georgia</td>
<td>No statistics *5</td>
<td>191</td>
<td>N/A *4</td>
<td>743</td>
<td>635</td>
</tr>
<tr>
<td>Moldova</td>
<td>No statistics *5</td>
<td>5,087</td>
<td>N/A *4</td>
<td>2,714</td>
<td>134</td>
</tr>
<tr>
<td>Nepal</td>
<td>No statistics *5</td>
<td>20,715</td>
<td>N/A *4</td>
<td>16,503</td>
<td>0</td>
</tr>
<tr>
<td>Norway</td>
<td>1,396</td>
<td>2,232</td>
<td>74,865</td>
<td>4,411</td>
<td>44</td>
</tr>
<tr>
<td>Spain</td>
<td>10,230</td>
<td>18,902</td>
<td>603,358</td>
<td>23,877*6</td>
<td>437</td>
</tr>
<tr>
<td>Sweden</td>
<td>1,395</td>
<td>788</td>
<td>782,291</td>
<td>2,306</td>
<td>162</td>
</tr>
</tbody>
</table>

* Please note, as explained in the text, that direct access is not included in the statistics.
*1 In Estonia, a direct access system is used. This figure has been provided by the Estonian authorities.
*2 This figure includes all requests for Subscription data. For other countries the corresponding figure only covers requests that are handled by authorized personnel, and automated requests that refer to a criminal case.
*3 This figure includes all requests to which we were not able to answer, most often because the requested information was about a customer not of our operations but of another operator.
*4 No automated emergency positioning system in use.
*5 Statistics are not available.
*6 This figure has been corrected. Due to an editing mistake, the October 2015 report wrongly read ’20,608’.
Authority requests*  
July 1 – December 31 2014

<table>
<thead>
<tr>
<th>Country</th>
<th>Lawful interception</th>
<th>Historical data</th>
<th>Emergency Positioning</th>
<th>Subscription Data</th>
<th>Challenged/ rejected requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denmark</td>
<td>2 606</td>
<td>612</td>
<td>231 685</td>
<td>4 308</td>
<td>4</td>
</tr>
<tr>
<td>Estonia</td>
<td>1862 *4, JAN-DEC</td>
<td>N/A *1</td>
<td>262 206</td>
<td>608</td>
<td>12</td>
</tr>
<tr>
<td>Finland</td>
<td>1 339</td>
<td>796 *2</td>
<td>128 419</td>
<td>1 985</td>
<td>16</td>
</tr>
<tr>
<td>Nepal</td>
<td>482</td>
<td>21 947</td>
<td>N/A *3</td>
<td>12 373</td>
<td>2</td>
</tr>
<tr>
<td>Norway</td>
<td>699</td>
<td>1 085</td>
<td>76 644</td>
<td>3 317</td>
<td>33</td>
</tr>
<tr>
<td>Spain</td>
<td>9 911</td>
<td>18 073</td>
<td>767 375</td>
<td>22 042</td>
<td>492</td>
</tr>
<tr>
<td>Sweden</td>
<td>2 236</td>
<td>959</td>
<td>1 023 788</td>
<td>1 816</td>
<td>99</td>
</tr>
</tbody>
</table>

*1 Historical data request are, for Estonia, included in ‘Subscription data’ as the separation of the two categories was not possible due to the internal reporting methods used in our operations in Estonia.  
*2 In this table, for Finland, IMEI requests were moved from ‘Historical data’ to ‘Subscription data’.  
*3 There is, in Nepal, no automated emergency positioning system in use  
*4 In Estonia, according to local laws and regulations, a direct access system is in place. This figure, therefore, has been provided by the authorities.

Authority requests  
1 Jan – June 31 2014

<table>
<thead>
<tr>
<th>Country</th>
<th>Lawful interception</th>
<th>Historical data</th>
<th>Emergency Positioning</th>
<th>Subscription Data</th>
<th>Challenged/ rejected requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finland</td>
<td>1 630</td>
<td>1 892</td>
<td>90 511</td>
<td>475</td>
<td>*</td>
</tr>
<tr>
<td>Sweden</td>
<td>1 145</td>
<td>995</td>
<td>1 605 949</td>
<td>1 284</td>
<td>*</td>
</tr>
</tbody>
</table>

Authority requests  
1 Jan – June 31 2013

<table>
<thead>
<tr>
<th>Country</th>
<th>Lawful interception</th>
<th>Historical data</th>
<th>Emergency Positioning</th>
<th>Subscription Data</th>
<th>Challenged/ rejected requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finland</td>
<td>3 570</td>
<td>4 091</td>
<td>81 038</td>
<td>1 623</td>
<td>*</td>
</tr>
<tr>
<td>Sweden</td>
<td>1 947</td>
<td>1 996</td>
<td>1 073 881</td>
<td>No figures</td>
<td>*</td>
</tr>
</tbody>
</table>

Definitions

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

By ‘historical data’ we mean historical traffic data, location data on mobile devices and cell-tower dumps. Traffic data
relates to the use of telecommunications services, including call data records, SMS records, and Internet records. These records include information such as the number of a called party, and the date, time and duration of a call. Internet session information includes the date, time and duration of Internet sessions as well as email logs. This figure also includes manual emergency positioning requests by the emergency centers and police.

By ‘emergency positioning’, reported up until June 2015, we mean positioning requests in emergencies from the emergency/rescue authorities (112 and other, Public Safety Answering Points). This report includes all positioning requests of automated emergency call positioning where emergency centers can directly generate a positioning request and immediately access the location of a mobile device.

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

‘Challenged/rejected requests’ contains information on how many requests we have challenged, for example by asking for clarification, the correction of formalities or rejecting the request. All requests from authorities must be legally correct. TeliaSonera 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.

**REQUESTS FROM AUTHORITIES**

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

### 3. Direct access without requests

Direct access without requests, technical systems for more extensive possibilities to monitor telecommunications (ex: mass surveillance by national security authorities)

### 4. Shut-down, blocking, restriction of access, etc

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

**Category 1:**

TeliaSonera Law Enforcement Disclosure Reporting on statistics. See this report, Chapter ‘Statistics, day-to-day requests from January 2014 to December 2015’.

**Categories 2 and 3:**

TeliaSonera has no insight into the extent of surveillance and cannot provide any statistics. TeliaSonera has, however, added a list of national legislation within these two categories to this Report, see below. Proposals for new laws or significant imposed operational changes in the area of these two categories may be defined as unconventional requests (‘major events’) within Category 4.

**Category 4:**

TeliaSonera reporting on unconventional requests and demands (‘major events’). See below in this report.
Unconventional requests and demands

TeliaSonera regards unconventional requests and demands from authorities which might potentially have serious impacts on the freedom of expression in telecommunications as ‘major events’. Governments’ requests or 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. The policy defines TeliaSonera’s commitments in relation to such unconventional requests or demands with potentially serious impacts on freedom of expression in telecommunications, such as direct network access, shutdown of networks and blocking of access to the Internet or specific websites. This is described in greater detail in the chapter ‘Definitions’ under the head-line ‘Requests from authorities’. We also include and address initiatives for new law-making which might potentially have serious impacts on freedom of expression as ‘major events’. Our commitments are published here.

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

It must be noted that the below indication of the number of major events during a specific period, is quite arbitrary. If in one country a large number of websites have been blocked, and in another country only one, then each counts as one major event in the figures below. A shut-down of the network or a service in part of a country is counted as a major event equally as a shut-down of the network or service in all of a country. A minor up-date of a system for government direct access to TeliaSonera’s networks and services, e.g. SORM, is counted equally as a much more substantial up-grade of such a system.

A. UNCONVENTIONAL REQUESTS AND DEMANDS 2013

In November 2013, we published the following on teliasonera.com: ‘Government requests in Eurasia as to major freedom of expression events’:

“So far in 2013 TeliaSonera has been asked to restrict access to the network and/or to certain web sites some 20 times in our Eurasia operation. In none of the cases had we been allowed to disclose the requests, should we have wished to do so, due to local laws and regulation on confidentiality. TeliaSonera aims to contribute to transparency by reporting on requests with serious impact on freedom of expression on our corporate website, to the extent possible. Examples of such requests are major shut-down of networks, mass surveillance, and blocking of access.”

B. UNCONVENTIONAL REQUESTS AND DEMANDS JANUARY TO JUNE 2014

Based on TeliaSonera’s freedom of expression policy adopted in December 2013, we have from January to June 2014 logged some ten major requests or demands from governments across our operations that have potentially serious impacts on freedom of expression in telecommunications.

These have been related to for instance closure of networks or services, blocking of content, new laws and/or significant imposed operational changes in relation to surveillance of communications.

TeliaSonera’s Group Policy on Freedom of Expression in Telecommunications focuses on requests or demands made by governments relating to the surveillance of communications. Such requests or 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. The policy defines TeliaSonera’s commitments in relation to requests or demands with potentially serious impacts on freedom of expression in telecommunications, such as unrestricted real-time network access, shutdown of networks and blocking of access to the Internet or specific websites.

In most cases, TeliaSonera promoted freedom of expression applying a practical point-of-challenge: such as requesting the decision to be put in writing or postponing implementation inasmuch as the law allows. On those occasions when we were required to suspend services, we did not say that this was the result of technical problems.

TeliaSonera aims to strengthen transparency by reporting on the receipt of requests or demands that have a
potentially serious impact on freedom of expression. However, only in a few of these cases have we been allowed to disclose the requests or demands due to local laws and regulations. In 2014 we have been able to communicate publicly on major issues related to freedom of expression in Latvia, Lithuania, Kazakhstan and Sweden.

Based on our Group Policy, we seek to influence legislation in relation to the surveillance of communications. To this end, we have held high-level meetings with decision-makers and influencers in a range of countries to present our position on the issues.

C. UNCONVENTIONAL REQUESTS AND DEMANDS JULY TO DECEMBER 2014

From July to December 2014, we have logged approximately some ten major requests or demands from governments across our operations with potentially serious impacts on freedom of expression in telecommunications. Most of these ten are new issues during the period, escalated to TeliaSonera.

A majority out of these some ten events are still open cases, e.g. on-going legislative initiatives or blocking activities, where we are pursuing our point of view.

In most cases, TeliaSonera promoted freedom of expression, e.g. by escalating the requests cover all from requests to transmit mandatory SMSs on a specific day and time, to legislative initiatives which are debated, lobbied and decided over a long period of time. Requests can also be escalated during the period July to December 2015, we closed some 20 unconventional requests or demands from governments across our operations. To support the decision making process and ensure a consistent view on policy commitments and requirements.

In most of the above some 20 cases, TeliaSonera has promoted freedom of expression, e.g. either and or by lobbying legislative initiatives, by publishing information about the demands (see case studies in the Chapter ‘Cases’ here below) as well as by requesting and pursuing blocking decisions to be put in writing in accordance with the rule of law. In some of these, TeliaSonera’s point of challenge might only have resulted in delay of the measure decided by the State. In a few cases TeliaSonera has so far not been able to perform any point of challenge other than efforts to assure the rule of law, e.g. by requiring and following-up that the unconventional request or demand is provided in writing.

Awareness-building and learning within the TeliaSonera Group is on-going, with the aim for all potentially major events to be assessed, escalated and logged.

A notable major event is the blocking of web-sites in Tajikistan. TeliaSonera has repeatedly reported about the developments on teliasonera.com.

D. UNCONVENTIONAL REQUESTS AND DEMANDS JANUARY TO JUNE 2015

From January to June 2015 our log contains the handling of approximately 20 unconventional requests or demands from governments across our operations, i.e. requests and demands with potentially serious impacts on freedom of expression in telecommunications, assessed and escalated to TeliaSonera Group. A handful of these were escalated already before 2015, but most of the 20 were new issues escalated during the first half of 2015. Some ten major events are in one way or another still open after June 2015. These are mainly on-going legislative initiatives or blocking activities but also requests as to direct access (e.g. SORM-systems).

As to SORM we are pursuing our point of view based on the Freedom of Expression Policy. In this context, it is valuable that the Policy has also been adopted by all of TeliaSonera’s local majority owned subsidiaries. As to requests for direct access, TeliaSonera has, however, challenges to push back, to promote freedom of expression. TeliaSonera acknowledges that the concept of what constitutes unconventional requests (‘major events’) may vary between geographies. To ensure that we have a common understanding of what our policy commitments mean in practice, to respect freedom of expression, there is a need for continued dialogue regarding e.g. why points of challenge are needed, the type of cases that should be escalated and how to reconcile license requirements with policy commitments and requirements.

In previous reports we have reported the approximate number of ‘logged’/’handled’ unconventional requests. We will from now on report on the approximate number of ‘closed’ unconventional requests. The reason is that unconventional requests cover all from requests to transmit mandatory SMSs on a specific day and time, to legislative initiatives which are debated, lobbied and decided over a long period of time. Requests can also be handled over a longer period of time due to the assessments and escalations performed by TeliaSonera.

During the period July to December 2015, we closed some 10 unconventional requests or demands from governments across our operations. To support the decision making process and ensure a consistent view on freedom of expression throughout the group, we facilitated local company risk assessments and escalations. Points of challenge, where possible, were defined jointly by local, regional and group management.

In about half of the some 10 closed cases, TeliaSonera promoted freedom of expression, e.g. by escalating the
requests and by publishing information about them on teliasonera.com/news (see case studies in the Chapter 'Cases' here below).

As to direct access, e.g. SORM and similar systems, we are pursuing our point of view based on the Freedom of Expression Policy. The main difference between direct access and other systems is the legal framework through which law enforcement agencies can monitor citizens. Whereas in many countries law enforcement agencies need to ask the telecommunications operator for assistance, in e.g. ex-Soviet Union republics the legal system often allows law enforcement agencies to bypass the telecommunications operator entirely via the SORM system of direct access. TeliaSonera has no way of knowing how often and for what purpose communications traffic is accessed, to what extent the rights of our users is interfered with. TeliaSonera therefore advocates that governments should not have direct access to our networks and systems, that TeliaSonera should retain operational and technical control. TeliaSonera has, as was reported in the October 2015 version of this report, challenges to push back and promote freedom of expression in this context. Several requests regarding SORM where handled during the end of 2015 and closed at the beginning of 2016. It is challenging to discuss and refer to specific requests for direct access publicly. Such requests are most often strictly confidential.

In one of our geographies it has proven difficult for the local company to receive the unconventional requests other than by e-mail although the law requires the requests to be in writing. TeliaSonera’s local company is trying to pursue its position visavi the authorities, i.e. that the requests must be sent on paper with a signature of the authorized official, even if in retrospect.

Awareness-building and learning within the TeliaSonera Group is continuing, with the aim for all potentially major events to be assessed, escalated and logged in a timely manner. Our ambitious goal is for all unconventional requests and demands to be challenged in some way or another in the perspective of TeliaSonera’s duty to respect the rights of users.
Laws providing governments direct access

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

What TeliaSonera can do is publish a list with links to such legislation in all of our respective markets. TeliaSonera aims to continue to update and publish the information below by reporting it bi-annually, to coincide with the publishing of the Annual and Sustainability Report (every March) and the sustainability update (every October).

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

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

In accordance with our freedom of expression policy, TeliaSonera advocates that governments should not have direct access to a company’s networks and systems. TeliaSonera should retain operational and technical control. TeliaSonera also advocates clear and transparent legal provisions on proportionality and necessity for all government surveillance of communications. Vague, non-transparent, and broadly conceived legal provisions are not appropriate when freedom of expression is at stake.

TeliaSonera has below listed, for markets in which we have majority owned operations, the most relevant laws on;

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

**MARKET** | **LEGISLATION**
--- | ---
Decree of the President, dated 02.10.2015, no link available

DENMARK | No signal intelligence and/or real-time access without requests in the legislation with the exception of that the Center For Cybersecurity may initiate lawful interception without a court order, but only if companies or governmental authorities have signed up for or requested this ad hoc. Telia Denmark is not a party to this arrangement and does not allow lawful interception without a court order.

ESTONIA | Electronical Communication Act (Elektroonilise side seadus) https://www.rigiteataja.ee/akt/4296/20140129
The relevant section is § 113 in Chapter 10.
FINLAND
No signal intelligence and/or real-time access without requests in the legislation. An official working party has concluded that there are needs for signal intelligence legislation in Finland and the Finnish government has the issue on its agenda but there is no bill proposal available at the moment.

GEORGIA
Law of Georgia on Personal Data Protection
Art. 2, paragraphs U, V, W
Art. 35,
Art. 55,
Criminal Procedure Code of Georgia
Art. 3, parts 31, 32, 33
Art. 143-143.10
Art. 327
Law of Georgia on Electronic Communications
Art. 2, definitions h_{6} – h_{63}
Art. 81 – 81, 82
Law of Georgia on State Secrecy
Art. 7, paragraph 4, sub-paragraph “a”

KAZAKHSTAN
Law on National Security, Art. 23:
http://adilet.zan.kz/rus/docs/Z1200000527
Law on Communication, Art. 8.1.17; Art 15, Art 21.3
http://adilet.zan.kz/rus/docs/Z040000567_
Law on Operative Investigative Activities, Art 11:
http://adilet.zan.kz/rus/docs/Z940004000_
Rules of interaction of bodies carrying out operative investigative activities, and organizations in the process of implementation and operation of SW/HW and technical facilities of conducting operative investigative activities on the telecom networks of the Republic of Kazakhstan, approved by Resolution of the Government of Kazakhstan #1593 dated December 23, 2011:
http://adilet.zan.kz/rus/docs/P1100001593
Technical Reglement "General requirements on security, functional and technical requirements to telecommunication equipment in the process of conducting operative investigative activities, approved Resolution of the Government of Kazakhstan #805, dated August 6, 2010:
http://adilet.zan.kz/rus/docs/P100000805_

LATVIA
1. The Electronic Communication Law (http://likumi.lv/doc.php?id=96611 ), Section 69 “Connection to Electronic Communications Networks”.
2. Cabinet of Ministers regulations No Nr.591 "Procedure for equipping electronic communication network for obtaining investigatory information from technical equipment and investigatory wiretapping of conversations in the cases specified by law" (unofficial translation).
Original language document:

LITHUANIA
Criminal Code of the Republic of Lithuania:
http://www3.lrs.lt/pls/interjidokpaieska.showdoc_flp_id=471480
http://www3.lrs.lt/pls/interjidokpaieska.showdoc_flp_id=494454
Code of Criminal Procedure of the Republic of Lithuania:
http://www3.lrs.lt/pls/interjidokpaieska.showdoc_flp_id=494449
Law on Criminal Intelligence of the Republic of Lithuania:
http://www3.lrs.lt/pls/interjidokpaieska.showdoc_flp_id=468203
Law on Intelligence of the Republic of Lithuania:
http://www3.lrs.lt/pls/interjidokpaieska.showdoc_flp_id=441110
http://www3.lrs.lt/pls/interjidokpaieska.showdoc_flp_id=494190
Publishing the above links to laws on direct access only does part of the job. In TeliaSonera’s view, customers should have easily accessible and user-friendly information on all surveillance legislation. Like statistics on the extent of surveillance, it is of course at first Governments who are to provide citizens with information about surveillance legislation. TeliaSonera and other players can however undertake to help make this information more accessible. This is why the Telecommunications Industry Dialogue has published a database covering 44 countries describing some of the most important surveillance powers available to government agencies and authorities seeking access to customer communications. Most of the information in the database has been provided by Vodafone and Telenor.
Industry Dialogue, of which TeliaSonera is an active member, has added reports on five countries so far, including Kazakhstan and Russia. We hope the database is useful to civil society organizations, academics, investors, and others who study the norms regulating government access to communications and their capacity to restrict content. TeliaSonera aims to continue to help building on this joint resource.

The database with information on surveillance legislation in, presently, 44 countries is available here; http://www.telecomindustrydialogue.org/resources/country-legal-frameworks/

A short video informing about the purpose and context of the database is available here; www.dustrydialogue.org/patrick-hiselius-explains-the-ids-resource-on-country-legal-frameworks/
Reported cases

Cases: Transparency as to specific unconventional authority requests

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

When it is possible to be transparent on some or all relevant information as to a specific major event, TeliaSonera does so by publishing articles on TeliaSonera.com/news. Here are the links to such articles from July through December 2015;

**UPDATES - Service limitations in Tajikistan**, 9 Oct 2014

**Mandatory distribution of SMS’s in Nepal**

**Request related to direct access in Tajikistan**, June 2015

**Blocking of a website in Nepal**

**New legislation in the country of Kazakhstan**

**Requests to Tcell to provide tools for surveillance**

CASE ON SHARED LEARNING: PUBLICLY SHARING TELIA SONERA’S UP-DATED TOOL FOR ASSESSING AND ESCALATING UNCONVENTIONAL AUTHORITY REQUESTS

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

Within TeliaSonera, such unconventional requests and demands are intended to be assessed and escalated in a way so that locally, regionally and group-wide, TeliaSonera can seek ways to respect freedom of expression. An internal tool for assessing and escalating was elaborated and updated during 2014, since adoption by TeliaSonera Group of the freedom of expression policy, based on learnings from actual major events. Contributing to industry best practice of shared learning, TeliaSonera published this internal tool, a form, on teliasonera.com in March 2015.

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

We also want to open up our tool for rights holder representatives and other stakeholders to comment upon our approach to help build the best possible process together. Based on additional learnings from actual major events we adopted and published a new version of the tool in March 2016.

The Form is available here;
Questions and Answers

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

By publishing Law Enforcement Disclosure Reports we want to make sure that our customers have access to information about that and to what extent government authorities have the power to access to data based on law and that TeliaSonera, according to our policies and procedures, protects our customers and with instructions to provide data to authorities only if and to the extent required to do so, or with the customers' permission. We also point out and link to legislation allowing the governments in most of our markets direct access to our systems and networks.

We encourage governments to be transparent about their use and scope of surveillance of communications. TeliaSonera’s advocacy is based on our Group Freedom of Expression Policy available here.

Which authorities were covered by the ‘Emergency Services’ statistics?
The statistics cover all local emergency services authorities such as the police, ambulance service, and fire brigades. With regards to Finland and Sweden for example the report covers the Emergency Response Center (Swedish: ‘SOS alarm’ and Finnish: ‘Hätäkeskuslaitois’) and Border Patrol Authority (Finnish: ‘Rajavartiolaitos’).

This report includes all positioning requests of automated emergency call positioning. Emergency centers can directly generate a request and immediately access the location of a mobile phone.

In Sweden, all mobile calls to 112 are located. In Finland, in addition to positioning of mobile calls to 112, the emergency center can also locate users that have not called 112, for example if a person goes missing.

How often will you publish a new report?
We publish a new Law Enforcement Disclosure Report every six months (bi-annually) including the total number of requests from authorities per country as well as links to laws providing governments’ direct access as well as information on major events covering the whole TeliaSonera Group.

In this fourth TeliaSonera Law Enforcement Disclosure Report we publish statistics covering requests from the police and other authorities regarding nine countries; Denmark, Estonia, Georgia, Moldova, Nepal, Norway, Spain and Sweden. Our aim is to add similar statistics from additional markets to the report in October 2016. TeliaSonera is considering which countries could potentially be added to the next report.

Do you ever challenge a request?
All requests from authorities must be legally accurate. The instruction is to reject or challenge any request that does not conform to the agreed form and process, for example when a form has not been signed or has not been sent by an appropriate sender. In such cases TeliaSonera asks for clarification.

As to ‘Major Events’, according to our Group Freedom of Expression in Telecommunications Policy, we have committed to and determined how to pursue a point-of-challenge when our customers’ freedom of expression and privacy is at risk in relation to unconventional requests or demands. This implies that we are to make careful assessments of all unconventional requests and demands that may have serious impacts on the freedom of expression. A strict escalation procedure for internal decision-making has been put in place to follow the policy. Formal decisions on the extent of compliance or refusal to comply with problematic requests or demands are not to be made at local company level, unless there are exceptional reasons.

Will you publish Law Enforcement Disclosure Reports on all countries?
In this TeliaSonera Law Enforcement Disclosure Report we publish statistics covering requests from the police and other authorities in nine of our markets. Our aim is to add similar statistics from additional markets to the report in October 2016. We will continue to analyze the legal situation in other countries and will aim for transparency in all our markets in the future, where practically possible and legally permissible.

However, it should be noted that there is an on-going challenge not the least because in some countries the law governing disclosure might remain unclear. In addition, in certain countries there are potential risks for our employees which arise from our commitment to increase public awareness of the legal powers and operating practices of governments within the area of surveillance. These can be acutely sensitive matters.

Why do the figures differ between countries?
There are several factors that make it difficult to compare statistics between countries. TeliaSonera has different market-shares in different countries, and this is probably reflected in the figures. Furthermore, TeliaSonera is privy to each local authorities’ working-methods and priorities in different countries, and these methods are likely to differ.
Also, within TeliaSonera, there are different working-methods in different countries. We work to streamline our operations.

It is also good to remember that the figures show the number of requests from authorities, not the number of individuals that have been targeted. Not even TeliaSonera as the operator and provider of the information has this knowledge. The number of requests is most likely larger than the number of individuals that have been targeted.

Also, in some countries, one request may include several targets.

According to our policies and procedures TeliaSonera is to disclose information to authorities only to the extent required by law or with the customer’s permission. This is a non-negotiable part of the way we operate. However, it should be noted within this context that governments also have direct access, i.e. signals intelligence and real-time access without sending requests to the operators. Regarding such direct access, TeliaSonera has no insight into the extent of surveillance and cannot provide statistics. What we can do is publish links to relevant such legislation in our respective markets, in the way we do in this report.

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

**How might Law Enforcement Disclosure Reports be used?**
TeliaSonera’s aim is to make it transparent to users and stakeholders to what extent governments’ access customer data. Our Law Enforcement Disclosure Reports might help getting a clearer picture of the norms governing surveillance and thus can be used in research and advocacy. We also encourage governments to be transparent about their use and scope of surveillance of communications.

**What are the main challenges associated with Law Enforcement Disclosure Reporting?**
It should be noted within this context, that governments also have direct access, i.e. signals intelligence and real-time access without sending requests to the operators. Regarding such direct access, TeliaSonera has no insight into the extent of surveillance and cannot provide statistics. What we can do is publish links to relevant such legislation in our respective markets, in the way we do in this report.

**How does TeliaSonera enforce its Policy and internal instruction and processes in this context?**
We have backed up our commitments to freedom of expression and privacy by publishing our internal form for processing of unconventional requests or demands from authorities. We also disclose, to the extent possible, information about such major events as they happen or else in more general workings in this Law Enforcement Disclosure Report. Our Freedom of Expression Policy is included in relevant employee training and, for our business area Eurasia also in our whistle-blowing mechanism (the TeliaSonera ‘Speak-Up Line’). The Freedom of Expression Policy is part of our internal oversight and accountability model. TeliaSonera is also conducting Human Rights Impact Assessments.
Scope

In August 2014, TeliaSonera published its first Law Enforcement Disclosure Report, providing information about the number of requests that TeliaSonera received from authorities in Finland and Sweden during 2013 and the first half of 2014.

The second TeliaSonera Law Enforcement Disclosure Report included statistics covering five additional countries referring to the second half of 2014.

In third report, we published statistics covering requests from the police and other authorities in Denmark, Estonia, Finland, Georgia, Moldova, Nepal, Norway, Spain and Sweden.

We plan to update our reporting twice a year to coincide with the publishing of the Annual and Sustainability Report (every March) and the sustainability update (every October). The table included in the report shows the number of authority requests in each country based on a court order or other legal demand by the police or other authority.

It is our view that national laws and regulations should determine the scope and mechanism of transparency reporting on government requests for access to customer data.

INCLUDED IN THIS REPORT

With regard to Denmark the statistics include figures regarding the police, secret police, customs and 112 emergency authorities.

With regard to Estonia the statistics include figures regarding the police, secret police, and customs.

With regard to Finland the statistics include the police, secret police, and customs. Also figures regarding tax authorities are included, since in Finland the police investigate economic crimes in cooperation with the tax authorities.

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

With regard to Moldova the statistics include figures regarding the following authority organizations:
- Ministry of Internal Affairs
- Ministry of Defense
- National Anti-Corruption Centre
- State Protection and Guard Service
- Security and Intelligence Service
- Customs Service
- Penitentiary Department of the Ministry of Justice

With regard to Nepal the statistics include figures regarding the following authority organizations:
- Metropolitan Crime division
- Central Investigation Bureau
- Anti-terrorist Department
- Crime Investigation Department
- Army Police Force
- Military Police Battalion
- National Investigation Department
- Narcotics Control Bureau
- CIAA (Commission for the Investigation of Abuse of Authority)
- Courts
- Revenue Control Department (Tax Authority)
- Home Ministry
- Police
- NTA (Nepal Telecom Authority).

With regard to Norway the statistics include figures regarding the police, and security police.

With regard to Spain the statistics include figures regarding police, secret police, and customs.

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

TeliaSonera has committed itself to a Policy on Freedom of Expression in Telecommunications. The Policy defines TeliaSonera's commitments in relation to unconventional requests or demands with potentially serious impacts on the freedom of expression in telecommunications. You can read about our commitments here. TeliaSonera has committed itself to informing stakeholders of such events whenever and to the extent appropriate and legally permissible.
Main goals, challenges and omissions

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

MAIN GOALS

Our goal with this Law Enforcement Disclosure Report, our transparency reporting in the context of surveillance, is to build user trust and winning the confidence of investors. We therefore;

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

We are also to take further steps to establish effective grievance mechanisms.

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

MAIN CHALLENGES

- Governments have direct access, i.e. signals intelligence and real-time access without sending requests to the operators. As to such direct access, TeliaSonera has no insight into the extent of surveillance and cannot provide statistics. What we can do is to publish links to relevant such legislation in our respective markets in the way we do in this report.
- With regard to category of lawful interception, the number of requests is most likely larger than the number of individuals that have been targeted. Pertaining to requests for cell tower dumps (i.e. requests that oblige TeliaSonera to disclose data about the identity, activity and location of any phone that connects to targeted cell towers over a set span of time) the number of affected individuals is larger than the number of requests. This makes the statistics difficult to interpret.
- Our aim is to add similar statistics from additional TeliaSonera markets to our upcoming reports. We therefore continue to analyze the legal situation in other geographies, aiming for transparency to the greatest extent possible in all our markets in the future. However, it should be noted that there is an on-going challenge in that in some countries the law governing disclosure might remain unclear. In addition, in certain countries, there might be potential risks for our employees which could arise from our commitment to increase public awareness of the legal powers and operating practices of governments in the area of surveillance, as these can be critically sensitive matters.

NOT INCLUDED IN THIS HERE REPORTING

Other than surveillance: TeliaSonera’s statistics do not include requests from authorities that have no role in lawful interception or other services obligated for operators, such as requests from competition authorities and national regulatory authorities. Also, the report does not cover information on TeliaSonera’s voluntary commitment to block child sexual abuse material based on a list from Interpol.

Requests or demands from private entities: TeliaSonera local companies are not to act upon requests or demands from private entities to remove, filter or restrict access to content. The exception is Child Sexual Abuse images where TeliaSonera has been working with the UK-based Internet Watch Foundation. TeliaSonera also actively participates in combating spam, viruses and denial of service attacks to protect our customers and networks.

Information on emergency positioning

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

Customer Privacy

This report covers TeliaSonera’s commitments as to freedom of expression and privacy interaction with law enforcement authorities. Our commitments as to customer privacy, which is not covered in this report, are defined in our Privacy Policy, available here. Our work to this regard is published in our October Sustainability Update report, as well as in the March Annual and Sustainability report.

TeliaSonera International Carrier operations

TeliaSonera owns and operates one of the largest fiber-optic networks in the world, providing network infrastructure and services to more than 3,000 customers in 80 different countries worldwide. TeliaSonera International Carrier markets are not included in the law enforcement disclosure statistics in this report.
Further information

REPORT ON LOCAL LAWS

The Telecommunications Industry Dialogue in June 2015 published a database with information on local laws, including TeliaSonera's markets; Sweden, Norway, Spain, Russia and Kazakhstan. The database is available here.

NEW VERSION OF THE TELIASONERA GROUP FREEDOM OF EXPRESSION POLICY

In September 2015 we updated our Group Freedom of Expression Policy. The new version is published here. The main additions compared to the previous version of the policy (dated 2013-12-05) are the following;

- In the chapters 'Description' and 'Purpose':
  "TeliaSonera has adopted this Policy’s principles to define our standards for _supporting and_ respecting the freedom of expression."

- In the chapter ‘Scope’: "TeliaSonera Group works towards adopting _and implementing_ this Policy’s principles and objectives in all other operations in which TeliaSonera has ownership interests."

- In the chapter ‘Scope’: "Such requests or demands addressed to TeliaSonera may relate to:
  ..._significant changes or_ proposed changes in the law, or significant imposed _or proposed_ operational changes, in the context of freedom of expression in telecommunications"

- In the principle 2: "We argue that all government surveillance of communications, _including international collaboration between authorities_, should be conducted under the supervision of a court or some other independent judicial body."

- In the principle 5: "We always strive to act in the best interest of our customers and the company. Risks to customers, _including children and youth_ relating to freedom of expression are integrated into our risk management process _to minimize possible negative impacts of government requests or demands_."

Adding a new chapter, ‘Roles and responsibilities’: Each Executive Vice President, Senior Vice President and Vice President reporting to the CEO of TeliaSonera is responsible for ensuring that this Group Policy is duly communicated and implemented, and that the employees within his/her area of responsibility are familiar with and follow this Group Policy. All TeliaSonera employees are however individually responsible for reading, understanding and following this Group Policy. Each employee is also encouraged to speak up and raise concerns about actual or possible violations of this Group Policy. Violations of this Policy can lead to disciplinary action up to and including termination."

- Adding a new chapter, ‘Exemptions’: If any TeliaSonera Subsidiary would like to adopt a corresponding Group Policy with exemptions from this Group Policy, such exemption(s) must be approved by the board of TeliaSonera.

GOVERNMENT LAW ENFORCEMENT DISCLOSURE REPORTS

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

Denmark:

Finland:
http://www.intermin.fi/download/58755_Selvitys_poliisin_tiedonhankinnasta_ja_vakuunnasta_vuonna_2014.pdf?3be464c58728f1288

Georgia:

Norway:
https://www.regjeringen.no/contentassets/tcf0734e8e221f478f77992c83ba461f3/dk-utv_aarsrapport_2014.pdf
and
http://eos-utvalget.no/norsk/arsmeldinger/content/text_1451994737474247247338f_rsmelding_for_2014.pdf

Sweden: