TeliaSonera Transparency Report, January2015

National authorities' collection of customer data in some of our markets

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

Maintaining customer privacy is of utmost importance to TeliaSonera: it is one of the pillars in our Group Code of Ethics and Conduct. At the same time, TeliaSonera – like all telecommunication's companies – is 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.

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.
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 the respective government regularly publicly reports to the Parliament about the scope of surveillance. Although these publications might not always cover all kinds of requests and demands, we see government reports as a good starting point for discussing the best practice for meaningful transparency, considering that a government can cover all telecom operators in any respective country.

Through its transparency reporting TeliaSonera wants to add to applicable government reports and 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 of the proper limits of government surveillance powers. We will therefore continue to publish transparency reports regularly every six months.

In this TeliaSonera Transparency Report we continue publishing statistics covering requests from the police and other authorities in Finland and Sweden. Starting January 2015, we disclose statistics for the second half of 2014 for Estonia, Denmark, Nepal, Norway and Spain. We will update our reporting twice a year. Our aim is to add similar statistics from additional TeliaSonera markets to our next Transparency Report, which is to be published in August 2015. We therefore continue analyzing the legal situation in other geographies, aiming for transparency to the greatest extent possible in all our markets in the future.

In addition to the reporting of statistics, we aim to report transparently on our efforts in relation to requests or demands with potentially serious impacts on the freedom of expression in telecommunications. We identify such exceptional and unconventional requests and demands as 'major events'.

Stockholm, January 30, 2015

Jonas Bengtsson

Senior Vice President and General Counsel, TeliaSonera

Transparency Report January-June 2014, July-December 2014 and full-year 2013

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 under the headline Requests from authorities, page 3.

It should be noted that there are several factors that make it difficult to compare the statistics between countries, see Q&A Section; 'Why do figures differ between countries'.

Authority requests 1 July – 31 Dec 2014					
Country	Lawful interception	Historical data	Emergency Positioning	Subscription Data	Challenged/ rejected requests
Denmark	2 606	612	231 685	4 308	4
Estonia	1862*[4] Jan-Dec	N/A *[1]	262 206	608	12
Finland	1 339	796*[2]	128 419	1 985	16
Nepal	482	21 947	N/A *[3]	12 373	2
Norway	699	1 085	76 644	3 317	33
Spain	9 911	18 073	767 375	22 042	492
Sweden	2 236	959	1 023 788	1 816	99

*[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 method 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 – 30 June 2014					
Country	Lawful interception	Historical Data	Emergency positioning	Subscription Data	Challenged/ rejected requests
Finland	1 630	1 892	90 511	475	*
Sweden	1 145	995	1 605 949	1 284	*

Authority requests 1 Jan – 31 Dec 2013					
Country	Lawful interception	Historical Data	Emergency positioning	Subscription Data	Challenged/ rejected requests
Finland	3 570	4 091	Jul-Dec 81 038	1 623	*
Sweden	1 947	1 996	Jul-Dec 1 073 880	No figures	*

* Reporting started July 2014

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). 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’ 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 phone.

By ‘subscription data’ we mean secret numbers and information about supplementary services. Subscription data refers to details which appear on a phone 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.

Major Events

TeliaSonera regards 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 or blocking or restricting of access to telecom services or networks. This is described in greater detail under the headline Requests from authorities, page 12. We also 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 ‘major event’ as soon as the specific event occurs, but 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 details. This is why we will publish aggregated information on ‘major events’ in parallel with our January and August transparency reports.

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.

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.

A. Major events, 2013

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

B. Major events, 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. Major events, 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. lobbying legislative initiatives and requesting blocking decisions to be put 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, here.

D. 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 surveillance and cannot provide any statistics. What TeliaSonera can do is to publish a list of relevant legislation in our respective markets. Such a list is published below.

First it must be noted 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 the respective country.

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 to assess the legality, necessity and proportionality of these measures. States should therefore be transparent about the use and scope of communications surveillance.

In accordance with our freedom of expression policy, 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.

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. Below TeliaSonera has listed the most relevant laws in markets in which we have majority owned operations 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 monitoring of telecommunications.

Market	Legislation
Azerbaijan	The Constitution of Azerbaijan Republic (the main law). Art. 32.4.. http://en.president.az/azerbaijan/constitution/ The Law on Operative crime detection activity. Art.10; 11; 12. http://e- qanun.az/print.php?internal=view&target=1&docid=2938&doctype=0 The Criminal-Procedural Code, Art. 177. http://e-qanun.az/print.php?internal=view&target=1&docid=14&doctype=1 The Law on Telecommunications, Art. 39. http://e-qanun.az/print.php?internal=view&target=1&docid=10663&doctype=0
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. http://fe-ddis.dk/cfcs/CFCSDocuments/Lovomcenterforcybersikkerhed.pdf.
Estonia	Electronical Communication Act (Elektroonilise side seadus) https://www.riigiteataja.ee/akt/129062014019 The relevant section is § 113 in Chapter 10.
Finland	No signal intelligence and/or real-time access without requests in the legislation. Currently there is an official working party evaluating possible needs for signal intelligence legislation in Finland.
Georgia	Law of Georgia on Personal Data Privacy

	Art. 2, paragraphs U, V, W *Art. 35[1]* *Art. 55[1]* *https://matsne.gov.ge/index2.php?option=com_ldmssearch&view=docView&id=1561437&impose=parallelEn* Criminal Procedure Code of Georgia *Art. 3, parts 31, 32, 33* *Art. 143[1] - 143[10]* *Art. 332[3]* *https://matsne.gov.ge/index2.php?option=com_ldmssearch&view=docView&id=90034&impose=parallelRu* Law of Georgia on Electronic Communications *Art. 2, definitions h[56] – h[62]* *Art. 8[1] – 8[2] - 8[3]* *https://matsne.gov.ge/index2.php?option=com_ldmssearch&view=docView&id=29620&impose=parallelRu* Law of Georgia on State Secrecy *Art. 7, paragraph 4, sub-paragraph "a"* *https://matsne.gov.ge/index2.php?option=com_ldmssearch&view=docView&id=33280&impose=parallelEnRu*
Kazakhstan	Law on National Security, Art. 23: http://adilet.zan.kz/rus/docs/Z1200000527 Law on Communication, Art. 15, Art. 8.1.17: http://adilet.zan.kz/rus/docs/Z040000567_ Law on Operative Investigative Activities: 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_ Uniform rules of interaction and centralized management of telecommunications networks, approved by Resolution of the Government of the Republic of Kazakhstan # 1499, dated December 8, 2011:http://adilet.zan.kz/rus/docs/P1100001499
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: http://likumi.lv/doc.php?id=114208
Lithuania	Criminal Code of the Republic of Lithuania: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=471480 Law on Criminal Intelligence of the Republic of Lithuania: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=468203 Law on Intelligence of the Republic of Lithuania: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=441110 Law on Electronic Communications of the Republic of Lithuania: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=463812

Moldova	Art. 20 of the Law on electronic communications: http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=327198 Art. 132(8) Criminal Procedure Code: http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=350171 Art. 7 of the Law on Intelligence Security Service: http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=311721 Art. 18 of the Law on special investigation activity: http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=343452
Nepal	No signal intelligence and/or real-time access without requests in the legislation.
Norway	https://lovdata.no/dokument/NL/lov/2003-07-04-83 Lov om elektronisk kommunikasjon, Section 6-2 a – (not translated) mobilregulerte soner. According to the Criminal Procedure Act: http://www.ub.uio.no/ujur/ulovdata/lov-19810522-025-eng.pdf
Spain	Spanish law does not appear to grant government agencies the legal powers to mandate direct access into a communication service provider's networks without the operational or control or oversight of the communication service provider.
Sweden	http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Lag-2000130-om-forsvarsunde_sfs-2000-130/ Additional information; http://www.fra.se/omfra/myndighetenfra/lagstiftning.123.html
Tajikistan	Law On Telecommunications, Art. 34 http://www.adlia.tj/base/show_doc.fwx?rgn=3249 http://ispa.tj/?p=34
Uzbekistan	Presidential Decree 513 On measures to increase effectiveness of organization of operative investigation measures on telecommunication networks: http://ict.gov.uz/rus/normativno_pravovaya_baza/ See document nr 8 under Section 3.Law on Telecommunications, Art. 18: www.lex.uz/Pages/GetAct.aspx?lact_id=33152

Questions and answers

Why is TeliaSonera publishing Transparency Reports?

Like all telecommunication operators, we are required by laws in the countries where we operate to assist authorities for purposes such as enforcing criminal law or assisting in emergency services. We only disclose customer information in accordance with the law and we assure the process to ensure it complies with the law.

By publishing Transparency Reports we want to make sure that our customers know that government authorities have access to data based on law and that TeliaSonera protects our customers and gives data to authorities only if required to do so or with the customers' permission.

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 are covered by the 'Emergency Services' statistics?

The statistics cover all local emergency services authorities, typically the police, ambulance service and fire brigades. As regards Finland and Sweden, for example, the report covers the Emergency Response Center (Swedish: 'SOS alarm' and Finnish: 'Hätäkeskuslaitos') 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 Transparency Report every six months, including the total number of requests from authorities per country as well as information on Major Events covering the whole TeliaSonera Group.

In this second TeliaSonera Transparency Report we publish statistics covering requests from the police and other authorities regarding seven countries: apart from Finland and Sweden, we have added Denmark, Estonia, Nepal, Norway and Spain. Our aim is to add similar statistics from additional markets to the Transparency Report in August 2015. TeliaSonera is now considering which geographies can be added to the August 2015 report.

Do you ever challenge a request?

All requests from authorities must be legally correct. TeliaSonera will 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', in 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 is at risk. This implies that we make careful assessments of all major 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 major problematic requests or demands are not made at local company level, unless there are exceptional reasons.

Will you publish Transparency Reports on all countries?

In this TeliaSonera Transparency Report we publish statistics covering requests from the police and other authorities in seven of our markets. Our aim is to add similar statistics from additional markets to the Transparency Report in August 2015. We will also continue analyzing the legal situation in other geographies, aiming for transparency in all our markets in the future where it is practically possible and legally permissible.

Why do the figures differ between countries?

There are several factors that make it difficult to compare the statistics between countries. TeliaSonera has different market-shares in different countries, and this is probably reflected in the figures. Furthermore, TeliaSonera does not know the authorities' working-methods and priorities in different countries, but the methods are likely to be different. Also, within TeliaSonera, there are different working-methods in different countries. We aim 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 we as the operator and provider of the information have this knowledge. Most likely, however, the number of requests is larger than the number of individuals that have been targeted.

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

Does TeliaSonera make money on this?

No. Local legislation often prescribes that the operators must finance the system set-up and that the authority has to compensate for every single request (cost-based).

How might Transparency Reports be used?

TeliaSonera's aim is to make it transparent to its users and stakeholders to what extent governments access customer data. Our Transparency Reports might help getting a clearer picture of the norms governing surveillance and thus 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 challenges associated with Transparency Reporting?

In some countries, governments have direct access to operator's networks and systems, which makes the statistics on the number of requests less valuable. In this second Transparency Report TeliaSonera has therefore included a chart with links to legislation providing such direct access.

Scope

In August 2014 TeliaSonera published its first Transparency Report, informing about the number of requests that TeliaSonera received from authorities in Finland and Sweden during 2013 and the first

half of 2014. This second TeliaSonera Transparency Report includes data about additional five countries in the second half of 2014.

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. Such data is usually requested by the police but also by other authorities, such as customs and tax authorities.

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

Included in this report

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

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

With regard to Finland the statistics include figures regarding the police, secret police, customs and 112 emergency authorities. Also figures regarding tax authorities are included, since in Finland the police investigate economic crimes in cooperation with the tax authorities.

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 police, security police, and emergency authorities.

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

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’), the Economic Crime Authority (Swedish: ‘Ekobrottsmyndigheten’) and 112 emergency authorities.

All requests from authorities must be legally correct. TeliaSonera will 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 TeliaSonera asks for clarification.

TeliaSonera has committed itself to a Policy on the Freedom of Expression in Telecommunications. The Policy defines TeliaSonera's commitments in relation to 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 appropriate and legally permissible.

Not included in this transparency reporting

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.

Not included in this Major Events report

As regards signals intelligence and real-time direct access, for example, TeliaSonera has no insight into the extent of surveillance and cannot provide any statistics. In this second Transparency Report TeliaSonera has therefore included a chart with links to legislation providing such real-time direct access.

Request 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.

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

1. Requests from law enforcement authorities:

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

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

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

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

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

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

3. Real-time access without requests, technical systems for more extensive monitoring of telecommunications (example: mass surveillance by national security authorities)

4. Shut-down, blocking or restriction of access (example: shut-down of SMS-communication, blocking of the whole Internet or of certain web sites)

Category 1:	TeliaSonera Transparency Reporting.
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. Proposals for new laws or significant imposed operational changes in the area of these two categories may be 'major events' within Category 4.
Category 4:	TeliaSonera reporting on 'major events'.

The international framework

The international framework that exists within the area of human rights and which TeliaSonera is obliged to follow is multifaceted. Freedom of expression and protecting the privacy of a telecoms operator's customers are essential rights that have a particular bearing on a telecoms operator's business.

It has become increasingly important for TeliaSonera and other operators to be able to respect these rights, as national authorities impose greater demands on the ability to monitor telecommunications and Internet traffic in order to safeguard national security and combat crime.

It is vital for TeliaSonera to have a good understanding of the limits of our responsibilities and how we can best address these issues. This is a challenge for the entire global telecommunications industry. For further information on the international framework on freedom of expression and privacy, see here.

TeliaSonera is an active participant in the 'Telecommunications Industry Dialogue on Freedom of Expression and Privacy'. The initiative, where the participating telecommunication companies share the best practices also as regards Transparency Reporting, is presented here.