**Question 1:**

Laws, regulations and other measures (including where applicable contractual arrangements and extra-legal action) that may permit the Norwegian authorities to require Telecommunications and Internet Service Providers to:

a) Suspend or restrict access to websites or Internet and telecommunications networks;

b) Provide or facilitate access to customer data.

**Answer to question 1:**

The Electronic Communications Act was adopted in 2003, and together with the

|  |
| --- |
| Regulations on Electronic Communications Networks and Services (Electronic Communications Regulations) sets out the framework for what the Norwegian authorities in the relevant sectors may require of national Telecommunications and Internet Service Providers. English translations of the laws and regulations can be found here: |

<http://eng.nkom.no/laws-and-rules> and here: <http://eng.nkom.no/laws-and-rules/regulations>

This legislation replaced the former Telecommunications Act and the regulations on public telecommunications networks and services, and it implements four directives adopted by the EU in 2002. These make up the EU’s regulatory framework for electronic communications networks and services. They have been incorporated into the EEA Agreement and entered into force for Norway on 1 November 2004.

a) There are currently no national laws or regulations that permit the Norwegian authorities to restrict access to specific websites or networks, but the internet filter ‘the Child Sexual Abuse Anti-Distribution Filter’(CSAADF) is a collaborative project between Kripos (the National Criminal Investigation Service) and Norwegian internet service providers (ISPs).

Use of this filter by ISPs is voluntary, and it involves the ISP redirecting traffic to a server in its own network instead of showing a website that displays child abuse content. All websites that are blocked are monitored by Kripos. The ISPs are responsible for the technical part of this access blocking and redirection. The criteria for blocking content are set out in sections 310 and 311 of the General Penal Code, which deal with presentations of a sexual nature that involve children. Originally, use of this filter was voluntary for end users, but the ISPs that are collaborating with Kripos now use it for all customers.

As the result of a District Court ruling against Telenor in September 2015, several of the main ISPs in Norway introduced a block on The Pirate Bay (TPB). Even though ISPs that have not been specifically referred to in the ruling have said that they will not block TPB, the block has been implemented using the same technology as the Kripos filter (DNS blocking). The web page that is shown when TPB is blocked is similar in many ways to the one that is shown when websites displaying child abuse content are blocked by the CSAADF.

b) Under section 2-9 of the Electronic Communications Act, providers and installers of electronic communication networks and services ‘have a duty to maintain secrecy regarding the content of electronic communications and third party use of electronic communications, including information on technical systems and procedures.’ Secrecy regarding third party use of electronic communications means, for instance, that information on traffic data is considered to be secret, as follows from section 7-1 of the Electronic Communications Regulations. In addition, information on the time of logging on or off, which IP addresses have been used for this, and information about when an email has been sent or received are all covered by the duty of secrecy, as are the IP addresses that can be linked to the electronic communications.

In certain cases, however, providers and installers of electronic communication networks and services are exempt from this duty of secrecy, and may provide the information mentioned without contravening section 2-9 of the Electronic Communications Act.

**In criminal cases:**

When carrying out investigations of criminal matters, the police may obtain various kinds of information about an individual’s use of electronic communications. Under section 118 of the Criminal Procedure Act, the Ministry may exempt a witness from the statutory duty of secrecy, so that they can give evidence in court. Similarly, a person may be exempted from the duty of secrecy under section 230 of the Criminal Procedure Act when required to make a statement to the police.

Authority relating to the duty of secrecy under the Electronic Communications Act has been delegated from the Ministry of Transport and Communications to the Norwegian Communications Authority. This means that the Norwegian Communications Authority makes independent assessments of requests submitted by the police or prosecuting authorities for exemptions to be granted from the duty of secrecy. In such cases the authority must strike a balance between the protection of privacy, the investigative needs of the police, and society’s interest in fighting crime.

Providers and installers must not be exempted from the duty of secrecy ‘when the revelation may be detrimental to the State or public interests or have unfair consequences for the person who is entitled to preservation of secrecy’ (section 118 of the Criminal Procedure Act). On this basis, Norwegian Communications Authority carries out an assessment of whether is it reasonable to make an exemption from the duty of secrecy, in line with the principles set out in section 170a of the Criminal Procedure Act on the use of coercive measures.

Under the Electronic Communications Act, section 2-9, third paragraph, providers and installers may give certain information directly to the police without seeking the consent of the Norwegian Communications Authority or being ordered to do so. This applies to information about ‘unlisted telephone numbers under an agreement or other subscription information, as well as electronic communications addresses’ (static and dynamic IP addresses). Under the Act, providers and installers can, in addition to providing unlisted telephone numbers, provide ‘other subscription information’, including personal data (e.g. names, addresses) connected to a subscription. This also includes information on which SIM cards can be linked to an IMEI number, information on which other SIM cards have been used in a particular terminal, which phone numbers can be linked to a SIM card, which SIM cards can be linked to charging session, irrespective of the charging method, and the IMSI number of a SIM card.

Given the way question 1 is formulated, traffic data and location data resulting from the use of a mobile phone must also be considered customer data. Under sections 7-1 and 7-2 of the Electronic Communications Regulations, providers and installers have specific obligations regarding the processing of traffic data and location data and what the information may be used for. Under section 7-1 of the regulations, processing of data traffic ‘may only be carried out by persons working with invoicing, traffic control, customer queries, marketing of electronic communications services or disclosure of illegal use of electronic communications’. It is in connection with these tasks that traffic data may be used, and ‘processing shall be restricted to that which is necessary for performance of specified work tasks’. Under section 7-2 of the regulations, location data that is not traffic data (i.e. signalling data) may only be processed by persons with authorisation from the provider of the electronic communication network or service, and this data is only to be processed in anonymised form. Apart from in the cases mentioned in sections 7-1 and 7-2 of the regulations, the relevant data may only be used if it is anonymised or the user has given his or her consent, cf. section 7-4 of the regulations.

**In civil cases:**

Under section 22-3 (2) of the Civil Disputes Act, the authority to consent to the presentation of evidence that is subject to a statutory duty of secrecy under the Electronic Communications Act in civil cases has been delegated from the Ministry of Transport and Communications to the Norwegian Communications Authority. These cases usually concern breaches of the Copyright Act, and the Norwegian Communications Authority carries out concrete assessments and seeks to strike a balance between the protection of privacy and the need to fully elucidate the case.

**Question 2:**

Laws, regulations and other measures (including where applicable contractual arrangements and extra-legal action) on the public disclosure of requests made or actions taken to (a) suspend or restrict access to websites and telecommunications networks and the requests to provide or (b) facilitate access to customer data.

**Answer to question 2:**

a) Please see the answer given to question 1 a). It is only Kripos and the relevant police authority that have access to information on the websites and domain names that are blocked by the internet filter CSAADF. This information is not available to the public.

b) Please see the answer given to question 1 b).

**In criminal cases:**

In criminal cases, there are a number of basic principles that safeguard the rights of suspects during the investigative stage and during criminal proceedings. For instance, there are a number of rules on securing and collecting evidence. These matters lie outside the Ministry of Transport and Communication’s area of responsibility.

For telecommunications, there are rules for listening in on (tapping) telephone conversations in real time. These rules can be found in section 216 a. of the Criminal Procedure Act. It is only the courts that have the authority to permit phone tapping. Under Chapter 16 a. and 16 b. of the Criminal Procedure Act, the courts may also permit the police to use other forms of monitoring of communications.

**In civil cases:**

The provisions of section 22-3, see the third and fourth paragraphs of section 28-3, of the Civil Disputes Act provide for access to information that is subject to a statutory duty of secrecy. The provisions of section 22-3 relate to the securing of evidence out of court and the prohibition against evidence subject to a statutory duty of secrecy, see section 2-9 of the Electronic Communications Act. Evidence may be secured ‘if it can be significant in a dispute to which the person who presents the petition may become a party or intervener, and there is either a clear risk that the evidence will be lost or considerably impaired, or there are other reasons why it is particularly important to obtain access to the evidence before a lawsuit is instigated’ (section 28-2 of the Civil Disputes Act). Paragraphs four to six of section 28-3 of the Act are applicable when ‘there is reason to fear that notice to the opposite party could obstruct the securing of evidence’. If the court considers this to be the case, it may decide that evidence can be secured before the opposite party is notified, and ‘neither the opposite party nor the public shall be informed of the case before the evidence is secured or more than six months have elapsed since the case was closed’.

**Question 3:**

Laws, regulations and other measures (including where applicable contractual arrangements and extra-legal action) governing the activities of private entities that provide network components or related technical support, such as network equipment providers, submarine cable providers, and Internet exchange points.

**Answer to question 3:**

Provided that a company or entity is covered by one of the definitions given in section 1-5 of the Electronic Communications Act, duties may be imposed under Chapter 2 and Chapter 8 of the Act. In particular, see section 2-1 on the duty to register, section 2-3 on requirements for network, service, associated equipment and facilities, section 2-9 on the duty of secrecy, section 2-14 on requirements for installers, and section 8-1 on the right to possess, sell and use radio and terminal equipment. An English translation of the Act can be found here: <http://eng.nkom.no/laws-and-rules>

**Question 4:**

Remedies available in the event of undue restrictions on Internet and telecommunications access or undue access to customer data.

**Answer to question 4:**

|  |
| --- |
| The provider and installer with universal service obligations under section 5-1 of the Electronic Communications Act is required to provide access to public telephone services and digital electronic communications networks to all locations with permanent year-round residents or businesses (normal delivery area). Currently, this provider is Telenor. A permanent year-round resident is anyone with a permanent postal address in the National Registry. Within the normal delivery area, Telenor is required to provide landline telephony under normal terms and conditions. Telenor can choose to offer wireless solutions at no additional cost to the consumer. These rules are set out in an agreement between the Ministry of Transport and Communications and Telenor (Norwegian only). |

The political authorities in Norway have decided not to introduce a universal service obligation for broadband. Norwegian telephone operators and internet service providers therefore do not have a duty to provide broadband, and consumers are not entitled to require access to this service.

**Question 5:**

Other relevant laws, policies or initiatives to promote or enhance Internet accessibility and connectivity, including measures to promote network neutrality.

**Answer to question 5:**

The Norwegian authorities have long advocated access to the internet as an important tool for promoting freedom of information and safeguarding fundamental human rights online, and ensuring open and democratic processes. Norway has put forward this position on many occasions in international forums such as the OECD, the International Telecommunication Union (ITU), the Council of Europe, the EU High-Level Internet Governance Group, the World Summit on the Information Society (WSIS), the Internet Governance Forum (IGF) and through its participation in

the Internet Corporation for Assigned Names and Numbers (ICANN) and the governmental advisory committee to ICANN, GAC. In all their international work, the Ministry of Transport and Communications and the Norwegian Communications Authority support the multi-stakeholder model of internet governance and enhanced cooperation based on the outcome documents from WSIS 2005 (the Tunis Agenda).

Since 2009, the Norwegian Communications Authority has also worked with actors in the Norwegian internet industry to develop guidelines for net neutrality. The overall objective of net neutrality has been to ensure that the internet remains an open and non-discriminatory platform for all types of communication and content distribution. The guidelines are currently not statutory, but there is nothing to prevent net neutrality being made a statutory requirement in Norway in the future, if the voluntary arrangement is no longer sufficient or common European rules are introduced.

The Norwegian guidelines for net neutrality are technology-neutral and apply to all types of access networks. They are based on three principles:

1. Internet users are entitled to an Internet connection with a predefined capacity and quality.

2. Internet users are entitled to an Internet connection that enables them to

* + send and receive content of their choice
  + use services and run applications of their choice
  + connect hardware and use software of their choice that do not harm the network.

3. Internet users are entitled to an Internet connection that is non-discriminatory with regard to type of application, service or content or based on sender or receiver address.

The guidelines are available in English here: <http://eng.nkom.no/technical/internet/net-neutrality/net-neutrality>