NORWAY – COUNTRY REPORT

Background

This report outlines the main laws which provide law enforcement and intelligence agencies with legal powers in relation to lawful interception assistance, the disclosure of communications data, certain activities undertaken for reasons of national security or in times of emergency, and censorship of communications under the laws of the Kingdom of Norway.

1. PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

1.1 Criminal Procedure Act 1981 ((LOV-1981-05-22-25) Lov om rettergang i straffesaker) (the "CPA")

According to section 216a CPA (which falls under chapter 16a on control of communications generally), the district court may make an order permitting the police to carry out communications surveillance when any person is, with just cause, suspected of attempting or committing an offence that:

- is punishable by imprisonment of 10 years or more; or
- contravenes certain provisions of the General Civil Penal Code (the "Penal Code") (a new version of which entered into force on 1 October 2015) including offences relating to national safety, political espionage, acts of war, and certain drug related crimes, or section 5 of the Export Control of Strategic Goods, Services and Technology Act 1987 (the "ECA"), which is a law dealing with export control and related offences.

"Communications surveillance" may consist of audio surveillance of conversations or other communications conducted to or from specific telephones, computers or other apparatus for electronic communication which the suspect possesses or which it may be assumed he will use. It may also, after an amendment in section 216a CPA in June 2016, consist of transmission of hidden signals to such apparatus for electronic communication as mentioned. This may result in surveillance of other phones than that of the suspect. The preparatory works of the amendments clarify that the police must, after having identified the suspect's phone, cease surveillance of other phones than that of the suspect.

The police may be empowered to conduct an interception themselves, or to order the owner or supplier of a network or service to provide such assistance as is necessary for carrying out the interception. The obligation to assist may apply either to the operator who owns the network used for the communication in question, or to the service provider that provides the communications service in question. The CPA does not identify the specific obligations of network operators or service providers, and the police have wide discretion to determine when assistance is necessary.

In addition, under section 222d CPA, the district court may make an order permitting the police to carry out communication surveillance pursuant to section 216a when there is just cause to suspect that someone will perform an act contrary to certain provisions of the Penal Code, which include offences relating to public safety, murder, robbery or organised crime.

Separately, section 222d CPA also provides that, where the Norwegian Police Security Service (the "PST") has reasonable grounds to believe that a person will commit an act that contravenes section 5 ECA, or certain serious crimes including threats to national security and terrorist financing as set out in the Penal Code, the measures set out in section 216a CPA may be invoked.

The PST is the police security agency of Norway and is responsible for monitoring and securing internal security. Publicly known operational departments include the counter-intelligence, investigation, surveillance and technology units.

Court orders issued to the PST may only be given by a judge with the relevant security clearance and the court order may only be issued by the district court chosen by the head of the Norwegian Supreme Court.

According to section 448 CPA, damages may be awarded to network operators and service providers for any loss caused as a result of requests for assistance by the police, when this is found to be reasonable by the court.

According to section 216d CPA, if there is a serious risk that an investigation will be prejudiced by delay, an interim order from the Norwegian Prosecuting Authority (the "NPA") may take the place of a court order. The NPA, which is part of the Norwegian Council of State (a decision-making body of senior government ministers), is responsible for legal prosecutions in Norway.

When the police issue a decision or request a court order, the decision must be made by the chief of police or deputy chief of police or, in their absence, certain other officials of the prosecuting authority as decided by the chief of police or the authorised deputy with written consent of the senior public prosecutor.

The interim order by the NPA must be submitted to the court for approval as soon as possible, and not later than 24 hours after the interception has begun. If the court considers that illegal interception has taken place, any evidence that has been uncovered will be treated in accordance with the rules on illegally acquired evidence.

According to section 216f CPA, permission for all types of control may not be given for more than four weeks at a time, and must not be longer than strictly necessary. If suspicion of an offence relates to a contravention of chapter 8 or 9 of the Penal Code (offences against the independence and security of the state and offences against the Constitution of Norway and the head of state) such permission may be given for up to eight weeks at a time. However, if an extension is required, the police must obtain a new court order (or a decision must be made by the PST or the NPA as per section 216d CPA).

In the summer of 2016, changes were made to the CPA that enable the police to access non-public information in computer systems, on the same terms as for regular communications surveillance.

According to the new section 216 O, the district court may make an order permitting the police to access non-public information in computer systems when any person is, with just cause, suspected of attempting or committing an offence that:

- is punishable by imprisonment of 10 years or more; or
- contravenes certain provisions of the Penal Code (including offences relating to national safety, political espionage, acts of war, and certain drug related crimes) or section 5 of the ECA.

Permission can only be granted when access is assumed to be of significant importance for solving the case, and that solving the case otherwise would be significantly impeded.

Permission can only apply to the accessing of specific computer systems or user accounts of network-based communication services or storage services controlled by the suspect, or accounts that are assumed to be used by the suspect. The access may include communications, electronically stored data, and other information regarding the use of the computer system or the user account.

In the new section 216 P, certain conditions are laid down regarding who may perform the actions necessary for the access specified in section 216 O, and which technical methods may be used. The access must be performed by qualified personnel under the direction of the police chief, the Police Security Service or other specifically authorised person. The Police may use hacking methods, installation of surveillance software, and carry out break-ins to install technical devices in order to carry out the access.

1.2 Police Act 1995 (Lov om politiet (LOV-1995-08-04-53)) (the "PA")

According to section 17d PA, the district court may – for a period of up to 6 months - make an order permitting the Police Security Service (the "PST") to carry out communication surveillance as set out in section 216a CPA, if there is reason to suspect that an offence under certain sections of the Penal Code will be committed. Such offences include terror offences, threatening national security or an offence against someone in the Royal Family, members of Parliament, the government, the High Court or representatives from similar institutions from other countries.

An order from the chief of the PST or his deputy may take the place of a court order if there is a serious risk of an offence against the Royal Family, members of parliament, the government, the High Court or representatives from similar institutions from other countries and preventative action would be impaired by delay.

2. DISCLOSURE OF COMMUNICATIONS DATA

2.1 Criminal Procedure Act 1981 ((LOV-1981-05-22-25) Lov om rettergang i straffesaker) (the "CPA")

According to section 216b CPA, the court may issue an order permitting the police to carry out other forms of control of communications, which may include requesting metadata for example, when a person is, with just cause, suspected of committing certain offences under the Penal Code that may result in imprisonment of five years or more. Such offences include acts that are a threat to national security, political espionage, terrorism, illegal access to data or programs or certain drug related crimes.

Control of communication includes:

- discontinuation or interruption of the transmission of conversations or other communications conducted to or from specific telephones, computers or other communication devices which the suspect possesses or it may be assumed he will use;
- requiring the owner or provider of the network or service which is being used for the communication to inform the police of which communication devices will, during a specific period of time, be linked or have been linked to the device specified in the first bullet point, and of any other data connected with the communication.

Under section 216c CPA, permission to carry out control of communications may only be given if it will be of substantial

significance to clarify the case and the use of other methods of investigation would be substantially more difficult.

The investigation control measure employed may consist of the police requiring that the owner or provider of the network service informs the police of traffic data and "other data". According to the preparatory works (Ot.prp.nr 64 (1998-99) section 23) of the section, "other data" may be but is not limited to:

- information about the duration of a call;
- the geographical location of a cell phone upon the time of the communication; or
- who was logged on to a computer at the time that the computer was used for communication purposes.

The police and the PST may also, following a court order, carry out control of communications in accordance with section 222d CPA, as described in section 1.1 of this report.

When the obtaining of a court order is likely to lead to a serious risk of delay, the police and the PST may apply for an interim order to be issued by the Prosecuting Authority, using the same procedure as is outlined in section 1.1 of this report in relation to interceptions.

2.2 Electronic Communications Act (Act No. 83 of 04 July 2003) (the "ECA")

Sections 2-7 ECA regulate how long and for what purposes network operators or service providers may retain metadata.

Traffic data must be deleted or rendered anonymous as soon as it is no longer necessary for communications or invoicing purposes, unless otherwise determined by or pursuant to law. Any other processing of traffic data requires the consent of the user.

2.3 Police Act 1995 ((LOV-1995-08-04-53) Lov om politiet) (the "PA")

According to section 17d PA, the district court may issue an order permitting the Norwegian Police Security Service (the "PST") to mandate the disclosure of communications metadata as set out in section 216b CPA and information from computer systems as set out in section 216 O, as well as carrying out other investigatory control measures, if there is reason to suspect that an offence under certain sections of the Penal Code will be committed. Such offences include terror offences, threatening national security or an offence against someone in the Royal Family, members of Parliament, the government, the High Court or representatives from similar institutions from other countries.

3. NATIONAL SECURITY AND EMERGENCY POWERS

In addition to the legislation set out above which makes reference to police powers in national security situations, specifically sections 216a, 216b and 222d of the Criminal Procedure Act 1981 and section 17d of the Police Act, the provisions set out below may provide government agencies with further powers in relation to national security and emergencies.

3.1 General Civil Penal Code (the "Penal Code")

According to section 17 of the Penal Code, no person will be punished for committing an act which would otherwise be an offence if they do so to save someone's person or property from what they believe to be an otherwise unavoidable danger. The circumstances must justify the extent of the act. The police have in some cases used this provision as the legal ground to, for example, jam signals, in instances not covered by the other powers outlined in this report.

In addition, under section 18 of the Penal Code, no person may be punished for an act committed in self-defence. As a result, an otherwise criminal act may be committed in defence against an unlawful attack if the act does not exceed what appeared to be necessary for that purpose. The act in self-defence must be proportionate to the danger of the attack, the guilt of the assailant or the legal right that is threatened by the attack.

Provided that the conditions in section 18 are fulfilled the provision may, for example, be used to block other frequencies than those that are part of a public communication network, as provided by section 6-2a ECA and section 216b CPA, for example, to trigger explosives.

3.2 Electronic Communications Act (Act No. 83 of 04 July 2003) (the "ECA")

According to the section 6-2a ECA, the police may use frequencies allocated to others through the use of "mobile regulated zones", subject to certain limitations.

Section 1-5, number 19 ECA defines a "mobile regulated zone" as a limited geographical area where communication in an electronic public communication network for public use is influenced or impaired by use of legal identification catching or jamming. Number 20 of the same section describes "identification catching" as the manipulation of networks used for public mobile communication for the purpose of uncovering the electronic identity of terminal equipment using the network.

The National Security Authority (the "NSA") may also, in exceptional cases and for a short period of time, use frequencies allocated to others without permission from the Norwegian Communication Authority (the "NCA") when this is a necessary measure for proper securing of conference rooms, cf. Section 16 of the Norwegian Security Act.

Both the police and the NSA must also notify the NCA without undue delay after the measure has been established if frequencies allocated to others are used.

The NCA decides, in consultation with the police or the NSA, if a network operator or service provider should be informed. If it is decided that a network operator or service provider should not be notified, this decision must be recorded and explained in writing. According to the preparatory works of the ECA

(Prop.69 L (2012-2013)) Endringer i ekomloven), the NSA and the police must balance the police's need for secrecy against the consequences for the network operator or service provider.

As a result of the use of mobile regulated zones, network operators or service providers may appear to experience irregularities in their systems. In order to avoid costly and unnecessary corrective actions, the police or the NSA will decide, on a case by case basis, whether the network operator or service provider should be informed that the irregularities may be due to the use of a mobile regulated zone. The decision is not subject to disclosure or appeal.

3.3 Ministry of Transport and Communication, public consultation regarding proposed changes to the Police Act and the Electronic Communications Act (Høring – forslag til endringer i politiloven og ekomloven – mobilregulerte soner mv.) (the "Consultation")

The Consultation proposes to amend section 6-1 ECA and section 7b PA. These amendments will give the police permission to establish mobile regulated zones in a greater number of scenarios than the law currently provides for, for example, to prevent serious disruptions of public peace and order or to prevent criminal actions with prison sentences of more than three years.

In addition, mobile regulated zones may be used to identify and block signals in networks other than just the public communication network, for instance, to block explosives that may be triggered by alarm systems or garage openers.

Network operators or service providers need not be notified if this is necessary to implement measures under the new section 7b. The decision not to notify network operators or service providers depends on a cooperative decision made by the police and the NCA, with the final word belonging to the police.

Furthermore, in certain situations the police will not be obliged to notify the NCA. This will only be applicable in a few special situations where there is a serious reason that makes it necessary to keep the police operation secret. If the new rules are implemented, the police will not have to obtain a court order to establish the mobile regulated zone. The decision may be made by the chief of police or the deputy chief of police.

The deadline for responding to the public consultation was 23 January 2015. As of 21 February 2017, no further developments had taken place.

4. CENSORSHIP

4.1 Constitution of the Kingdom of Norway (the "Constitution")

Censorship is prohibited under Article 100 of the Constitution. Certain laws do, however, provide government agencies with powers to block communications in specific circumstances, as set out below.

4.2 Criminal Procedure Act 1981 (Lov om rettergang i straffesaker (LOV-1981-05-22-25) (the "CPA"))

As set out in section 2.1 of this report, according to section 216b CPA, the district court may make an order permitting the police to carry out other forms of controls of communications when a person is, with just cause, suspected of committing certain criminal acts. The control may be exercised by discontinuing or interrupting the transmission of conversations or other communication conducted to or from specific telephones, computers or other communication devices that a suspect possesses or which it may be assumed that he will use.

The communication device must be identified, for instance by a telephone number or IP-address, in the court order. If communications to and from a specific IP addresses are to be blocked, the IP address, must be specific to that computer. If, for example, the computer is given a new IP address each time it connects to the Internet, the IP address is not suitable to identify that computer and the network operator or service provider cannot be ordered to block access to that IP address.

The police must be able to demonstrate a possibility that the device will be used based on objective criteria.

5. OVERSIGHT OF THE USE OF POWERS

5.1 The Communications Control Committee (Kontrollutvalget for kommunikasjonskontroll) (the "Committee")

In relation to the various police powers mentioned above, the Committee must verify that the police's use of their control of communication powers occurs within the confines of the law and that the use of these powers is minimised as much as possible, for example, by ensuring they are only used when necessary for an investigation.

The legal basis for the Committee's authority comes from chapter 2 of the Statute Regarding Communication Control 2000 (the "Communication Statute") and section 216h of the Criminal Procedure Act 1981 (the "CPA").

The Committee evaluates reports from the chief of police to the Office of the Public Prosecutor. It also evaluates any complaints from persons or organisations that claim to have been subject to illegal forms of control of communication. The Committee may also, at its own initiative, look into any case or matter in relation to the police's and the prosecuting authority's use of control of communication. The Committee does not evaluate on-going cases at the request of the prosecuting authority.

According to section 13 of the Communication Statute, the Committee must consist of three members and one or more deputies and the leader of the Committee must fulfil the requirements of a High Court judge.

Under section 17 of the Communication Statute, if the Committee finds reason to criticize the police or the NPA, the matter must be reported to the Attorney General and the Ministry of Justice.

5.2 The Norwegian Parliamentary Intelligence Oversight Committee (EOS-komiteen) (the "EOS Committee")

The EOS Committee is responsible for external and independent control of the Norwegian secret services (including the Police Security Service) (the "EOS Services"). The EOS Committee's primary task is to make sure that the EOS services keep their activities within the legislative framework applicable to them and must further ensure that no individual is subjected to unjust treatment. They must also ensure that the EOS Services do not make use of more intrusive methods than necessary under the circumstances.

The EOS Committee has seven members, including the Chair and Deputy Chair. The activities of the EOS Committee are subject to the Act relating to the Oversight of Intelligence, Surveillance, and Security Services of 3 February 1995 no. 7 (the "Oversight Act"). Provisions in the Oversight Act are supplemented by the Directive relating to the Oversight of Intelligence, Surveillance and Security Services of 30 May 1995 no. 4295, as determined by the Norwegian Parliament.

The EOS Committee submits a report on its activities to the Norwegian Parliament every year. Under Section 8 of the Oversight Act these reports cannot be classified. Prior to submitting the report to the Norwegian Parliament, the EOS Committee verifies that the requirements for releasing the document without classification have been met, by forwarding it to the EOS services involved. Statements in relation to complaints must also be unclassified. Information regarding whether any person has been subjected to surveillance activities will be classified, unless otherwise decided. Statements to administration will be classified according to their content.

6. PUBLICATION OF AGGREGATE DATA RELATING TO USE OF GOVERNMENT POWERS

Restrictions on network operators and service providers

The government does not have the legal authority to prevent a network operator or service provider from publishing aggregate data in relation to the volume of requests from the government it receives relating to the powers described in this report.

Aggregate data published by government agencies

As far as we are aware, the government does not publish aggregate data relating to its use of the powers described in this report.

7. CYBERSECURITY

7.1 Act relating to the Protection of Personal Data (Personopplysningsloven) (the "PPD") and the Regulation on Protection of Personal Data (Personopplysningsforskriften) (the "RPPD")

The PPD and RPPD are both based on the EU Directive 95/46EC and will be replaced in May 2018 with the implementation of the General Data Protection Regulation (the "GDPR"). Also note that the Act on Human Rights (Menneskerettsloven) incorporates the European Convention on Human Rights (the "ECHR") into Norwegian law, particularly where Article 8 (the right to respect for private and family life) becomes highly relevant for the purposes of data protection legislation.

Security breaches and the use of information systems in breach of established routines shall be treated as deviations of cybersecurity legislation as per Section 2-6 RPPD. If a deviation results in the unauthorised disclosure of personal data that is subject to the laws of confidentiality, the entity affected by the deviation is under an obligation to notify the DPI as per the third paragraph of Section 2-6 RPPD. An example of where this obligation would be triggered would be where there has been a hacking of an entity's customer database, which has consequently exposed the personal information of the entity's customers and put them at risk of identity theft.

Individuals must be notified of any situation that has caused their personal data to be unlawfully disclosed, according to case law from the Privacy Appeals Board (Personvernnemnda). How this notification is given must be decided taking into account the severity of the breach, the sensitivity of the data and the potential consequences for the individuals affected.

The Data Protection Inspectorate (Datatilsynet) (the "DPI") is responsible for monitoring and supervising compliance with the both the PPD and RPPD. To do so, the DPI has the ability to:

(a) under Section 44 PPD, demand the disclosure of information without paying regard to the duty of confidentially. The DPI may additionally demand access to sites where personal data registers are placed, sites where the processing of personal data takes place and access to the tools used for such data processing; and

(b) under Section 46.4 PPD, order that the processing of data in violation of the PPD or RPPD shall be stopped, or set specific conditions before the processing of the personal data can continue.

Decisions made by the DPI may be appealed to the Privacy Appeals Board which acts as an independent appeals body. Decisions of the DPI may also be brought before the regular courts of Norway for the purposes of appeal.

The penalties for non-compliance with the PPD include:

- fines issued by the Data Protection Authority of up to NOK 925 760;
- coercive fines issued in accordance with Section 7-2d of the Act on Enforcement; and
- criminal prosecution by the Norwegian Prosecution Authority, which may result in the imposition of fines or a maximum 1 year imprisonment.

7.2 Act relating to Protective Security Services ("Sikkerhetsloven") (the "PSS")

The PSS applies to public entities and to any legal person who

is a supplier of goods or services to an administrative agency in connection with a classified procurement.

Section 29 PSS lays down several conditions that are applicable to public entities proposing to procure critical infrastructure, which is defined under the Act as "facilities or systems necessary to maintain basic needs and functions of society". Specifically, Section 29 sets down obligations on such public entities to carry out risk assessments in relation to their cybersecurity systems and to notify the superior Ministry if a procurement may result in the establishment of an activity that poses a threat to security. In these latter types of cases, the King in Council may decide that the procurement shall be stopped, or that the risk shall be mitigated by outlining certain conditions for the procurement to adhere to before it may proceed.

The main responsibility for monitoring and supervising compliance with the PSS is held by the National Security Authority ("Nasjonal sikkerhetsmyndighet") (the "NSM"). The NSM is to be provided with unhampered access to any area where there is sensitive information or a sensitive object held, insofar as necessary for implementing their supervisory functions.

Pursuant to the first paragraph of Section 5 PSS, an agency regulated by the PSS must notify the superior Ministry or the Ministry of Defence if they have information concerning a planned or on-going activity that may cause a "non-insignificant" risk for any activity that poses a threat to security.

It is the King in Council who may make the necessary decisions to stop a planned or on-going harmful activity that is threatening security ("sikkerhetstruende virksomhet") from continuing. Examples of such activity include the preparation, attempt or execution of espionage, sabotage or terrorist acts. Such decisions are made in line with the second paragraph of Section 5A PSS and are enforceable in accordance with Chapter 13 of the Act on Enforcement ("Tvangsfullbydelsesloven"). This section was described as a "security vent" when initially being drafted, meant only for use in extraordinary circumstances. It is therefore meant for use in only rare and serious cases due to the fact that it provides the King in Council with wide powers. The means chosen to deal with the planned or on-going harmful activity threatening security shall not be more burdensome than what is necessary taking into account the risks at hand.

There is no appeal mechanism in place under the PSS for an individual or entity aggrieved by a decision made by the King in Council. If an individual or entity wishes to appeal such a decision, they must file a case with the Norwegian courts.

Failure to comply with the PSS may result in criminal prosecution resulting in an imprisonment sentence of up to six months under Section 31, unless the acts are punishable under stricter legislation (typically the General Civil Penal Code).

7.3 Act relating to Electronic Communications (Act No. 83 of 04 July 2003) (the "ECA")

The ECA applies to providers of electronic communication networks or services. The Act is monitored and supervised by the National Communications Authority (Nasjonal kommunikasjonsmyndighet) (the "NCA"). Providers of electronic communication networks or services are under a duty pursuant to Section 10-3 to disclose information to the NCA that is necessary for the implementation of the ECA or decisions made in accordance with the ECA.

Where there is particular risk of a cybersecurity breach and if a cybersecurity breach could damage or destroy a subscriber's or user's retained data or infringe their data protection, the provider of the electronic communication networks or services shall immediately notify the subscriber or user of this risk. Notification to the subscriber or user is not necessary under Section 2-7 ECA where the provider can show the NCA that satisfactory technical protective measures have been carried out for the data affected by the security breach.

In ensuring compliance with the ECA, the NCA may;

(a) order providers of electronic communication networks or services to implement restrictions on the use of their networks and services in the interest of national security or other important societal considerations. Pursuant to Section 2-5, providers shall also, without an order from NCA, implement necessary restrictions on the use of their networks or services in emergency situations that involve serious threats to life or health, safety or public order or danger of sabotage against networks or services;

(b) issue regulations on the duty of confidentiality and make case-by-case decisions, pursuant to the fifth paragraph of Section 2-9 and the second paragraph of Section 2-10, to ensure that providers implement measures that provide proper secrecy and preparedness to any data they hold. Note that providers of electronic communication networks and services have an active duty under Section 2-9 in any event to maintain secrecy/confidentiality regarding the content of their electronic communications, and any third party use of their electronic communications). Providers also have a duty to ensure the preparedness and availability of their electronic communications; and

(c) make spot checks, measurements and any other checks without prior notice to the provider under Section 10-1.

The powers of the NCA do not have any significant adverse effects on an individual's rights to privacy and a fair trial.

Decisions made by the NCA can be appealed under Section 11-6 to the Ministry of Transport and Communications.

According to Section 12-4, a breach of the ECA may result in a criminal prosecution resulting in liability to a fine or an imprisonment sentence of up to 3 years.

8. CYBERCRIME

8.1 The General Civil Penal Code ("Penal Code")

On October 1 2015, Norway's new Penal Code entered into force. The new code has several provisions relevant to cybercrime, with Chapter 21 on the protection of information and communication containing more specific provisions directly aimed at the prevention and prosecution of such crimes.

The main cybercrimes covered by the Penal Code are as follows;

Statutory Reference	Offence	Penalty
Section 201 Penal Code (This section implements Article 6 of the European Council Convention of 23.11.2001 on Cybercrime)	Creating, acquiring, possessing or making available: (a) passwords or other information that may give access to information systems or computer systems; or (a) software or anything else particularly designed for committing crimes directed at information systems or computer systems with the intention of committing a criminal act.	Fines or up to one year imprisonment.
Section 204 Penal Code	Breaking a protection or by any other means gaining unauthorised access to a computer system. (Note that this provision relates to the unauthorised access itself. Further unauthorised use of the system, such as searching for, changing or deleting data, will be covered by other provisions, such as the provisions in Chapter 28 on vandalism and damage to property).	Fines or up to two years imprisonment.
Section 205 Penal Code	Violating the right to private communication, by: (a) the use of a technical device to secretly intercept or record conversations between others, or negotiations in closed meetings to which the person does not participate himself, or which he has accessed without authorisation; (b) breaking protection or in another unjustified manner accessing information transferred by electronic or other technical means; (c) opening letters or closed written messages addressed to others, or by other means gaining access to such messages; or (d) hindering or delaying the reception of a message by hiding, changing, destroying or withholding the message.	Fines or imprisonment of up to 2 years.
Section 54 of the Act relating to Intellectual Property Rights (the "IPR")	Violation of copyright.	Fines or imprisonment of up to 3 years. (Note that violations of copyright are generally investigated and prosecuted by the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim).

In addition to the above, Chapter 21 IPR contains provisions for the prevention of crimes such as identity theft, unauthorised access to TV-signals, violation of trade secrets and violation of duty of confidentiality.

Compliance with the Penal Code is regulated by the Norwegian police and the Norwegian Prosecution Authority on the basis of the rules set down in the Act relating to Criminal Procedure.

The territorial reach of the Penal Code is set down in Sections 4 to 8. Section 7 is the important provision for hacking activities carried out by non-nationals abroad. In accordance with Section 7, criminal acts that are carried out abroad can be considered to have been carried out in Norway, if the act has had effect or was meant to have effect in Norway. Accordingly, hacking activities carried out by non-nationals and directed at Norwegian citizens or entities in Norway may be prosecuted in Norway in accordance with Norwegian law.

Decisions and judgements made in accordance with the Penal Code can be appealed pursuant to Part 6 of the Criminal Procedure Act to the relevant court of appeal.

8.2 Future legislation: Digital Border Defence (Digitalt grenseforsvar) (the "DBD")

In September 2016, a public committee appointed by the Ministry of Defence delivered their report which made recommendations on the establishment of a Digital Border Defence. This proposed system, which will be administered by the Norwegian armed forces' secret services, will enable the secret services to intercept all data flow through cables to and from Norway.

Even though access to information gathered through the Digital Border Defence will be supervised by a judicial process in the courts, the initiative is highly controversial and has been subject to extensive criticism by, among others, the Data Protection Inspectorate. The report has been out on public consultation, and is currently under evaluation by the Ministry of Defence for the potential proposal of new legislation. The initiative is likely to be the subject of extensive debate before any legislation is adopted by Parliament (Stortinget).

Law stated as at 21 February 2017.