telenor group

AUTHORITY REQUESTS FOR ACCESS TO ELECTRONIC COMMUNICATION – legal overview

MAY 2015

CONTENTS

* these countries are covered in other reports, see 'Introduction'

INTRODUCTION

INTRODUCTION

This document provides an overview of the most common kinds of laws which compel the Telenor Group to give government authorities access to customer communications in ten of the countries in which Telenor operates. The remaining three markets are available in other publications[1].

Whilst the laws themselves are all publicly available, in practice they tend to be little known and not well understood by the public. By publishing this document Telenor aims to increase transparency in this space to its customers and other stakeholders.

These laws include those that compel us either to divulge information about our customers and their communications to certain government authorities, typically secret intelligence services and law enforcement agencies, or to prevent or suspend access to certain content or services.

These types of laws are primarily devised to investigate or prevent crime and terrorism, and to safeguard national security and public safety. The government bodies that use these laws to obtain information from telecommunications network operators and service providers such as Telenor assert that such information is vital to the performance of their duties.

THE DIFFICULTY OF REPORTING ON THE LAWS

Compiling a summary report of the most commonly used laws for each of Telenor's markets has been a difficult and challenging task.

The detail and scope of the laws in question varies greatly between the different countries in which Telenor operates, reflecting our presence in Europe and in Asia. The laws themselves are all too often opaque and poorly written. As such, they can be hard to interpret, even for legal specialists.

In many countries the laws were originally conceived in the late nineteenth or early twentieth centuries to allow police or intelligence agencies to intercept and read letters and telegraphs, and place wiretaps on telephone landlines. Concepts and terminology appropriate for this earlier era do not easily fit into the context of today's world of smartphones, the internet and social media.

There is a notable lack of consistency in even the most fundamental legal terms and concepts. Some governments have constrained powers that limit the impact on an individual's rights to privacy and freedom of expression; others use much wider-ranging powers with substantially greater human rights impacts. Some of the statutes in question are lengthy and contain carefully expressed checks and balances. Others are only a few pages long, with unchecked and sweeping powers set out in a few short sentences.

In this document, we provide a country-by-country insight into the nature of the local legal regime governing law enforcement assistance.

OUTLINE OF THE TYPES OF LAW FEATURED IN THE REPORT

Lawful Interception

Most countries have laws that enable government authorities to order companies that provide communication services and/or operate telecommunications networks (CSPs) to allow the interception of their customers' communications. For example, to listen to a phone call, or to read an email. In practice, this means that the CSPs have to configure their own systems to give one or more government agencies real time access to the contents of communications.

The nature of the access that the CSP is obliged to give to its own network can vary greatly from one country to another. As the most intrusive form of government access, it is common for interception to be lawful only if a warrant has been issued for it and presented to the CSP in question. In some countries, limited access is granted on a case by case basis following the issuing of such a warrant by a court or public prosecutor. In others, the CSP must allow permanent direct access to its network with no control or visibility over the interception activities that the government in question carries out.

Disclosure of communications data

Every communication over a telecommunications network automatically generates certain kinds of technical data within the network itself. This metadata, at its simplest, is the information that the network needs in order to route the communication between sender and recipient.

We shall refer to such metadata as "communications data" in this report. It is often described as the 'who, where, when and how' of a communication. Importantly, it does not include the content of a communication. Communication includes the sending of data between computer servers, so communications data would include the IP address assigned to a device making or receiving a communication.

Because an analysis of communications data can reveal a large amount about an individual's movements and their social and professional relationships, it is regarded as an extremely useful resource for government agencies undertaking any form of investigation. Coupled with the fact that the disclosure of

[1] Hungary and India are covered in Vodafone's Law Enforcement Disclosure Report – Legal Annexe http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html and Pakistan will be covered in an upcoming report by the Telecommunications Industry Dialogue on Freedom of Expression and Privacy

communications data has traditionally been regarded as less of an invasion of privacy than intercepting a communication, almost all countries have laws that enable government agencies to require CSPs to disclose significant amounts of communications data to them.

As with interceptions, the forms that such disclosure can take and the degree of legal scrutiny or other oversight surrounding it vary greatly from country to country. In some legal jurisdictions, a government agency may have direct access to any communications data that it wants. However, it is more common to find some degree of legal process or oversight, though a warrant may not necessarily be required to accompany each disclosure request. Many countries also allow access to communications data in 'threat to life' scenarios, for example where a person has gone missing and the geo-location data of their mobile phone may indicate their location.

National security

Safeguarding national security is a fundamental duty of every government. As such, those government agencies charged with protecting and investigating threats to national security tend to be given greater legal powers than those given to law enforcement bodies. This is particularly true in relation to legal powers relating to interception and to disclosure of communications data, where intelligence agencies tend to be given a greater degree of discretion than law enforcement agencies.

In many countries, the definition of what constitutes a threat to national security is set out in detail in legislation dedicated to national security or intelligence matters. This specificity helps circumscribe the powers of, for example, the domestic intelligence services. In other countries, the scope of national security powers is wider. This often means that the distinction between the powers that law enforcement bodies have to access data to investigate crimes, and the powers that intelligence agencies have to investigate threats to national security, is less clear.

Emergency or crisis powers

Many countries have legislation that gives extraordinary legal authority to the government during periods of national emergency or crisis. These types of laws are typically drafted with natural disasters, wars and widespread civil disorder in mind. The laws generally enable government agencies to assume direct control of certain essential national infrastructure for the duration of the emergency, including telecommunication networks.

In some countries, the legislation names the CSPs whose networks may be taken over. In others, the government can choose to take control of any CSP's network. Emergency legislation of this type tends to be (but is not always) tightly controlled, for example requiring parliamentary approval for its use.

Powers to restrict web browsing or order network or service shut-down

This report also identifies legislation which allows governments to block a CSP's network or services. These tend to be laws that either restrict the CSP from allowing users to access certain kinds of online content or that allow the government to shut down the CSP's entire network or (more commonly) particular services (for example, temporarily suspending a mobile phone network or an instant messaging service in a particular city during a riot).

In terms of IP address blocking, many countries have laws that enable government authorities to order CSPs to prevent access to certain kinds of illegal or offensive content by anyone using their network. Typically, the scope of what constitutes illegal content is limited in the relevant legislation either to that depicting criminal offences such as child abuse or murder, or to websites offering activities that are illegal in the country in question (a common example is online gambling). The laws generally include the ability of the government to maintain an updated list of certain IP addresses and websites that must be blocked.

In other countries, illegal content is defined more broadly. Sometimes the definition of illegal content includes websites offering commentary that, for example, is critical of the government or of particular religious or ethnic sensitivities. In such cases the legislation, in effect, gives the government the power to censor public discussion of certain subjects.

In terms of the laws that enable shut down or suspension of a CSP's network or particular service, these are typically drafted to assist law enforcement agencies in tackling civil disorder, such as riots.

BANGLADESH – 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 law of the People's Republic of Bangladesh

PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

Bangladesh Telecommunication Regulatory Act, 2001 (the "BTRA")

Section 35 BTRA requires every telecoms service provider to have a licence in order to operate, and its provisions apply to all such licence holders. There is no definition of a "telecoms service provider" in the BTRA. However, the definitions of "telecommunication" and "telecom service" are widely drawn, covering users and service providers in connection with telecommunication services and apparatus.

Section 97(Ka) BTRA (as introduced by the Bangladesh Telecommunications (Amendment) Act 2006) is the sole statutory basis from which the government derives its powers in relation to surveillance and censorship, as outlined below.

Under section 97(Ka) BTRA, on the grounds of national security and public order, the government may empower certain government authorities (intelligence agencies, national security agencies, investigation agencies, or any officer of any law enforcement agency) to suspend or prohibit the transmission of any data or any voice call, and record or collect user information relating to any subscriber to a telecommunications service. This widely drafted provision encompasses interception capabilities. The relevant telecoms operator must provide full support to the empowered authority to use such powers. The BTRA does not provide for any time limits on these powers. As a result, an interception may last for as long as the agency implementing the interception decides.

Under this section "government" means the Ministry of Home Affairs, and approval for use of the powers this section is given by the Home Minister or any Minister appointed with the duty of the Ministry of Home Affairs.

Information and Communication Technology Act 2006 (the "ICT Act")

The ICT Act regulates the use of digital security certificates, the provision of data services and defines a series of offences related to malicious activity online. It provides remedies for offences such as unauthorized damage to computer systems, tampering with computer source code, hacking, publishing fake, obscene or defamatory information in electronic form, and publishing false digital signature certificates.

The ICT Controller is an officer appointed under the ICT Act and regulates its implementation. Under section 29 of the ICT Act, the Controller, or any officer authorised by him should investigate any contravention of the ICT Act, or the rules or regulations made under it. In order to do so, the Controller or authorised officer has the same powers as those vested in a civil court under Bangladesh's Code of Civil Procedure, which include powers of discovery and inspection and compelling the production of any document.

Under section 30, the ICT Controller may access any computer system, any apparatus, data or any other material connected with a computer system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to the computer system. The ICT Controller may, by order, direct any person in charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

Under section 46 of the ICT Act, if the ICT Controller feels that, in the interests of the sovereignty, integrity, or security of Bangladesh, international relations, public order or for preventing incitement to commission a legally recognised offence, it is necessary or expedient, they can direct any government agency to intercept any information transmitted

through any computer resource. In addition, they may order the subscriber or any person in charge of a computer resource to provide all necessary assistance to decrypt the relevant information. The reasons for undertaking such a measure must be recorded in writing.

However, telecoms operators are only bound to cooperate with an order from the authorities which has been authorised under section 97(Ka) BTRA (as set out above).

DISCLOSURE OF COMMUNICATIONS DATA

Bangladesh Telecommunication Regulatory Act, 2001 (the "BTRA")

There is no direct reference in the BTRA to storage of metadata. In general, storage of data relating to customers is likely to be a condition of a telecommunication operator's individual licence, which commonly requires operators to store metadata for a specified period of time. As billing is done on a monthly basis, operators need to store metadata for subscribers at least for a sufficient period so that the subscribers may make enquiries or seek an itemised bill before payment.

Under the broad powers granted in section 97(Ka) BTRA, on the grounds of national security and public order, the government may require a telecommunications operator to keep records relating to the communications of a specific user. However, when considering whether to give a retention request, the relevant government agency would need to consider the technical resources and capabilities of the operator to retain information.

Information and Communication Technology Act 2006 (the "ICT Act")

Telecommunications operators are required to provide any metadata as evidence if ordered to do so by any civil court. Accordingly, the ICT Controller or any person authorised by him can seek metadata when exercising the investigatory powers provided under section 29 of the ICT Act for the purpose of discovery and inspection, enforcing the attendance of any person and examining him on oath or affirmation, compelling the production of any document, and issuing commissions for the examination of witness for any offence committed under the ICT Act.

NATIONAL SECURITY AND EMERGENCY POWERS

Bangladesh Telecommunication Regulatory Act, 2001 (the "BTRA")

Under section 96 BTRA, the government may, on the grounds of public interest, take possession of any telecommunication system, and all arrangements that are necessary for operating it. It may continue such possession for any time period and keep the operator and his employees engaged on a full-time basis or for a particular time for the purpose of operating such apparatus or system. The government is obliged, however, to pay proper compensation to the owner or the person having control of the radio apparatus or the telecommunication system which it takes over.

Under section 97 BTRA, when a foreign power declares a state of war, or creates a warlike situation against Bangladesh or when there is an internal rebellion or disorder, or in a situation where the defence or security of Bangladesh or any other urgent state-affair needs to be ensured, the government will have priority over the operator or any other user regarding the use of a telecommunication system.

Moreover, if the President of Bangladesh declares a state of emergency, the government may suspend or amend any licence or certificate or permit issued under the BTRA, or suspend any particular activity of, or a particular service provided by, an operator.

Section 97(Ka) BTRA, as outlined in the sections above, is also applicable in states of emergency or national security.

Furthermore, section 66(Ka) BTRA (incorporated by the Bangladesh Telecommunications (Amendment) Act 2006) empowers the Bangladesh Telecom Regulatory Commission (the "BTRC") to stop any signal, message or request from any subscriber (where it is expedient to do so), in the interest of the sovereignty, integrity, or security of Bangladesh, international relations, public order or for preventing incitement of a legally recognised offence. Operators must assist the BTRC to implement this order.

Telegraph Act 1885 (the "1885 Act")

It should be noted that some relevant sections of the BTRA's predecessor, the Telegraph Act 1885 (the "1885 Act") are also still in force. However, no operating licences are currently issued under the 1885 Act. As a result the following provisions are no longer used, though we mention them for the sake of completeness:

Section 5 of the 1885 Act provides that, in the case of a public emergency or in the interest of public safety, the government or any officer authorised by the government, may take temporary possession of any telegraph established, maintained or worked by any person licensed under this Act.

Under the 1885 Act the government or authorised officer may order that any message or class of messages to or from any person or class of persons (relating to any particular subject) sent or received by any telegraph, may be blocked, intercepted or detained by, or disclosed to, the Government or an officer thereof mentioned in the order.

CENSORSHIP

Bangladesh Telecommunication Regulatory Act, 2001 (the "BTRA")

It should be noted that the national security-related powers granted under s97(Ka) BTRA discussed above in section 3.1 could, at least in theory, be used for the purposes of censorship.

Information and Communication Technology Act 2006 (the "ICT Act")

Under section 45, the ICT Controller (explained above) may issue an order to a licence-holder under the ICT Act to take certain measures or cease certain activities as specified in such order, if necessary to ensure compliance with the provisions of

the ICT Act, or rules and regulations made under it.

Under sections 57 and 59 of the ICT Act, if any person deliberately publishes or transmits, or causes to be published or transmitted, on a website or in any electronic form any material which:

(i) is fake or obscene; or

(ii) would lead to (or create the possibility of leading to) a deterioration in law and order; or

(iii) would prejudice the image of the State; or

(iv) would or may hurt religious belief; or

(v) instigate against any person or organisation,

this activity will be regarded as an offence, and the ICT Controller may make an order to block the communication flow.

OVERSIGHT OF THE USE OF POWERS

There are no oversight mechanisms mandated in law in relation to the above legislation. However, the government and the Bangladesh Telecom Regulatory Commission may exercise oversight.

The empowered law enforcing agency may bring a claim against any non-compliance with the rules mentioned above and there are stipulated penalties for first time, second time and third time failures.

PUBLICATION OF AGGREGATE DATA RELATING TO USE OF GOVERNMENT POWERS

Restrictions on network operators and service providers
There is no direct statutory restriction on publishing aggregated data on government requests for surveillance and censorship powers described above. However the Bangladesh Telecom Regulatory Commission may declare such data to be confidential, exercising its discretion under section 85(1) of the BTRA.

In addition, as the powers are exercised on the grounds of national security and public order, any information relating to the use of such powers is considered confidential information as it may be part of an investigation or used in judicial proceedings. An equivalent position is adopted under the Right to Information Act 2009, under which any information that is given in confidence to any law enforcement agency is excluded from publication under the scope of the Act.

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.

Law stated as at 31 January 2015.

BULGARIA – 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 Bulgarian law.

PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

Law on Electronic Communications 2007 (the "LEC")
Article 304 states that undertakings which provide public electronic communications networks and/or services must ensure that they are set up in a way which allows for interception of electronic communications in real time and real time access to data related to a specific call. Where this data cannot be provided in real time, the data should be provided to the State Agency for Technical Operations and to the State Agency for National Security as soon as possible after the termination of the call. The interception procedure should be carried out in accordance with the Law on Special Intelligence Means.

Subject to Article 305, the undertakings which provide public electronic communications networks and/or services provide, commission and maintain, at their own expense, one or several interception interfaces by which intercepted electronic communications can be transmitted to the facilities of the State Agency for Technical Operations and of the State Agency for National Security. In addition they must ensure that they are set up in a way which allows for transmission of intercepted electronic services to these facilities over fixed or switched lines. The technical parameters, configuration and conditions for maintenance of the interception interfaces should be coordinated with the State Agency for Technical Operations and approved by its Chairman.

Interception must be conducted in a way which excludes the possibility of illegal interference in, and ensures protection of, the information related to the interception. Intercepted electronic communications are received only by the State Agency for Technical Operations and by the State Agency for National Security in compliance with the Law on Special Intelligence Means (Art. 309).

General Requirements for Provision of Public Electronic Communications (the "Requirements") (issued in 2008)
The Requirements were issued by the Commission for Communications Regulation. In accordance with Article 19 of the Requirements, the undertakings that provide public electronic communications networks and/or services are obliged to cooperate for the safeguarding of public interests, defending national security and ensuring electronic communications for defence needs and in national emergencies (crises).

In pursuance of this obligation and depending on the network used or services provided by a particular undertaking, it is obliged to set conditions, at its own expense, for interception of electronic communications by providing interfaces for the needs of the national security and public order. For the purposes of complying with these obligations, undertakings cooperate with competent state authorities, such as the State Agency for National Security, and implements the relevant interfaces that transmit electronic communications to these agencies.

Law on Special Intelligence Means 1999 (the "LSIM")
The LSIM sets out the terms and conditions, procedures for use and application and the control related to the use of special intelligence means (which includes interception and other ancillary covert activities) and the results obtained via these means. Under the LSIM, special intelligence means are used to prevent or detect intentional severe crimes, as listed in Article 3 (such as spying, sabotage and murder), where the relevant circumstances cannot be established in any other way or would be disproportionately difficult to establish by any other means.

The following government authorities have the right to request the use of special intelligence means and to use the data collected and the material pieces of evidence retained: the National Police Directorate General, Organized Crime Fighting Directorate General, Border Police Directorate General, Internal

Security Directorate General, the specialized directorates (with the exception of Technical Operations Directorate) and the territorial directorates of the State Agency for National Security, and the regional directorates of the Ministry of Interior, Military Information and Military Police services with the Minister of Defence and the National Intelligence Service. For some specified crimes, requests can also be made by prosecutors from the relevant Regional Prosecutor's Offices (Article 13).

Interception under the LSIM can only be undertaken where there is a credible written request from the heads of these authorities or by a supervising prosecutor. The requests should contain certain statutory conditions (such as facts substantiating the view that a severe crime has been committed, the proposed time period for the use of interception, and activities undertaken so far in the investigation). The request should be submitted to the Chairman of the Sofia City Court, of the respective district court or of the specialized criminal court or to a deputy empowered by that Chairman who will authorize or refuse the use of special intelligence means (Article 14 and Article 15). In addition and unless there are exceptional circumstances, once the use of special intelligence means has been authorised by the relevant court, the chairman of the State Agency for Technical Operations issues a written order for enforcing the relevant special intelligence means.

Interception may only be conducted by the relevant departments of the State Agency for Technical Operations or the Technical Operations Directorate of the State Agency for National Security, in accordance with the LSIM. However, in a limited number of cases, interception may be conducted by the National Intelligence Service and by the intelligence services of the Ministry of Defence – in the sphere of their competence and by the Ministry of Interior – where an undercover officer of the Ministry participates in a relevant investigation of crimes where the use of special intelligence means is permitted (Article 20).

Penal Procedure Code 2006 (the "Code")

Pursuant to Article 172(3) of the Bulgarian Penal Procedure Code, computer information service providers (a term which encompasses communication service providers) are under an obligation to provide assistance to the court and pre-trial authorities in the collection and recording of computerized data through the use of special intelligence means (including interception). The use of special intelligence means is limited to the purposes of investigating intentional severe crimes (those for which the law provides punishment by imprisonment for more than five years, life imprisonment, or life imprisonment without substitution, such as spying, sabotage and murder), where the relevant circumstances cannot be established in any other way or would be disproportionately difficult to establish by any other means. Interceptions under the Code are conducted pursuant to the LSIM.

Under the Code, where interception is required in a pre-trial investigation, a credible written request for the use of special intelligence means is made by the supervising prosecutor to the court. The administrative head of the relevant Prosecutor Office making the request is also notified. The request should contain the following information listed in Article 173:

(a) information about the crime, the investigation of which requires use of special intelligence means;

(b) a description of the activities conducted within the investigation so far and the results thereof (so that the judge can assess if interception is the only remaining method available to collect data and evidence);

(c) information relating to the individuals that will be the subject of the interception;

(d) information on the operational investigative methods (that the request is for interception);

(e) the time period for use of interception (this is as a rule two months, but can be extended to six months); and

(f) the reasons why this method must be employed, and why the information required cannot be acquired in any other way, or that there would be extreme difficulties related to acquiring it in another way.

Authorization of the request is given by a ruling of the Chairman (or explicitly authorized deputy Chairman) of the respective court. On the grounds of the authorization, the Head of the State Agency for Technical Operations (or an authorized deputy head), or the Head of the State Agency for National Security (or an authorized deputy head) or the Chief Secretary of the Ministry of Interior, may issue a written order for the interception to take place.

Law on the Ministry of Interior 2006 (the "LMI")

The LMI provides that, for activities related to prevention, investigation and documentation of crimes and safeguarding the public order, the investigative bodies of the Ministry of Interior are authorized to collect, store and process information. "Information" is not defined and may therefore be widely interpreted. The process of gathering information includes control over communications in networks or separate communicational channels (Article 10, paragraph 2). These activities are carried out using special intelligence means (i.e. under the rules of LSIM), including interception.

Law on the State Agency for National Security 2008 (the "LSANS")

The LSANS sets out the statutory basis that, in carrying out their various investigative activities, the structures of the State Agency for National Security are authorized to use special intelligence means (including interception) in accordance with the LSIM (Article 123). Furthermore, they are authorized to require other state authorities, legal entities (such as companies) and individuals to provide the information necessary to carry out their obligations and such entities and persons are required to immediately provide any information that has been obtained or acquired in relation to a request

made in pursuance of the powers of the State Agency for National Security (Article129). There is no definition of "immediately".

DISCLOSURE OF COMMUNICATIONS DATA

Law on Electronic Communications 2007 (the "LEC")
Undertakings providing electronic communications networks and/or services have statutory obligations to keep safe the confidentiality of communications. However, due to the prevailing public interest, the LEC provides for three specific types of disclosure of communications data: (a) interception under the procedures of LSIM as this includes the provision of communications data related to the intercepted communication; (b) provision of information under Article 310 of the LEC (which would be requested prior to carrying out the interception); (c) disclosure of retained data. The specific cases under (b) and (c) are not related to disclosure of the content of communication.

The relevant details with respect to the interception obligation have been mentioned in Section 1.1 above. Pursuant to Article 310 of the LEC, before implementation of lawful interception takes place, the State Agency for Technical Operations and the State Agency for National Security require the undertakings that provide public electronic communications networks and/ or services to provide:

(a) data to establish the identity of the subscriber, the number or another identification feature of the electronic communications service;

(b) information about the service and the characteristics of the electronic communications system used by the subject of interception and provided by the undertakings that provide public electronic communications networks and/ or services; and

(c) information about the technical parameters of the transmission to the facilities of the State Agency for Technical Operations.

In addition, the undertakings that provide public electronic communications networks and/or services must retain, for a period of six months (which may be extended by a period of up to three months by permission of the court), certain data generated or processed in the course of their activities, which can be used to trace and identify the source of a communication, its destination, the date, time and duration of the communication, the type of the communication, the communications terminal equipment of the user or what purports to be a communications terminal equipment of the user, and the location label (Cell ID) (Article 251b). Pursuant to Article 251b, paragraph 3, other data, including data disclosing the content of the communications, may not be retained in accordance with this data retention procedure.

Access to the data retained is limited to the needs of national security and for the prevention, detection and investigation of serious crimes.

The retained data may be accessed by the authorities listed in Art. 251(c) (such as certain departments of the State Agency for National Security, the Ministry of Interior and the Ministry of Defence, as well as the National Intelligence Service) when such data is necessary for the performance of their duties.The retained data is accessed only after a credible court order is given by the Chairman of the respective regional court (or a judge authorised by him).

Alternatively, for the purposes of criminal investigations and proceedings under the Penal Procedure Code, the data are provided to the pre-trial investigation authorities and the court in compliance with such Code.

Penal Procedure Code 2006 (the "Code")
Article 159a sets out the procedures for accessing the data retained under the LEC for criminal investigations and proceedings under the Code. Under the Code, access to the retained data is granted by the undertakings providing electronic communications networks and/or services either upon request of the court (when the relevant proceedings are in their court stage), or on the credible order of a judge from the competent first instance court, issued under a substantiated request of the prosecutor supervising the pre-trial procedure (during the pre-trial stage). Such data may be accessed for the purpose of investigating severe intentional crimes.

NATIONAL SECURITY AND EMERGENCY POWERS

Law on Electronic Communications 2007 (the "LEC")
In accordance with Article 301 of the LEC, the undertakings that provide public electronic communications networks and/ or services, must ensure the capability for the provision of electronic communications in case of natural disasters as defined by the Disasters Protection Act, and in case of a declaration of a state of martial law, state of war or state of emergency in the meaning of the Law on Defence and Armed Forces of the Republic of Bulgaria.

In order to safeguard national security, undertakings which provide electronic communications networks and/or services must ensure the competent authorities have access to the network and/or the services provided, as well as the ability to use electronic communications over the network free of charge in case of an imminent threat to national security. In addition, if there is an imminent threat to national security or in a limited number of specified scenarios (detecting, identifying and defusing explosive devices and explosive substances; freeing hostages; detecting and preventing the use of national radio spectrum against the state etc.), the competent authorities may block the use of electronic communications services by using technical means, provided that the competent authorities in this case are the State Agency for National Security, certain bodies of the Ministry of Interior and National Security Office.

In accordance with Article 302 if a state of martial law or a state of war is declared, the Commission for Regulation of Communications (following a decision of a competent

authority) can temporarily suspend the validity of permits for radio spectrum frequencies. When such decisions are made the regulator is authorised to forbid the use electronic equipment or radio frequency spectrum for civil needs.

Where martial law, a state of war or a state of emergency has been declared, the terms and procedure for ensuring electronic communications shall be established by the Council of Ministers under the proposal of the Minister of Transport, Information Technology and Communications in coordination with the relevant competent authorities.

Subject to Article 17, the Minister of Transport, Information Technology and Communications is given broad powers to ensure the continued provision of electronic communications networks and services for the purposes of managing natural disasters (as defined by the Disasters Protection Act) and following any declaration of a state of martial law, state of war or a state of emergency (each as defined by the Law on Defence and Armed Forces of the Republic of Bulgaria).

Disaster Protection Act 2006
In accordance with Article 30, the undertakings which provide electronic communications have the obligation to assist the Ministry of Interior and the National Emergency Call System 112 to carry out communications during natural disasters.

Law on Defence and Armed Forces in the Republic of Bulgaria 2009
When a state of war, state of martial law or a state of emergency has been declared, the state authorities and the armed forces may take control over the facilities of the critical statutory infrastructure. The critical statutory infrastructure and activities are defined and identified by Decree No 181 of the Council of Ministers, dated 20th of July 2009 for determining of the strategic objects and activities critical for national security, where amongst other things, mobile and fixed communications services are determined as such activities. Three of the undertakings which provide such services (Mobiltel, Bulgarian Telecommunications Company and Telenor Bulgaria) are identified as part of the critical statutory infrastructure, meaning that the relevant state authorities and the armed forces may take control over their facilities (Article 123).

Law on the Ministry of Interior 2006 (the "LMI")
The police authorities may issue orders to state authorities, organizations, legal entities and natural persons where this is necessary for performance of their functions. As a general principle the orders are in writing, unless it is impossible to do, so long as they are understandable by the persons to whom the order is directed. The orders have minimum content determined by the law and are subject to appeal (Article 64). Furthermore, in the process of detection, identification and deactivation of explosive devices and explosive substances, police authorities may block electronic communications by using technical means (Article 90).

CENSORSHIP

The right of expression, regardless of the media used, is a fundamental right set out in the Bulgarian Constitution, and censorship is illegal (Article 39 and Article 40 of the Constitution of the Republic of Bulgaria). There are, however, a number of statues which provide for the blocking of certain information in particular circumstances, as set out below.

Law on Electronic Communications 2007 (the "LEC")
In specific scenarios, the competent bodies within the Ministry of Interior, the State Agency for National Security and the National Security Office may block, by technical means, the use of electronic communications services (Article 301, paragraph 3). These scenarios include but are not limited to the following: detecting, identifying and defusing explosive devices and explosive substances; freeing hostages; detecting and preventing the use of national radio spectrum against the state and when national security is threatened.

In addition, upon declaration of a state of martial law or a state of war and following the decision of a competent authority, the Communications Regulation Commission may suspend the validity of issued permits for radio spectrum frequencies and prohibit the use of radio equipment and radio spectrum for civil needs (Article 302).

Law on Electronic Commerce 2006
On the grounds of Article 15(b) and Article 16, paragraph 2 (related to providers of caching or hosting services), the providers of information society services must either delete the information stored in the course of provision of the services or block access to such information pursuant to an order of a competent authority. The law does not specify the meaning of "competent authority", however this would likely be interpreted to encompass all authorities with the power to lawfully require or implement blocking of access to content or those engaged in investigation and prevention of crimes, such as, the police at the Ministry of Interior, or the State Agency for National Security.

Law on the Ministry of Interior 2006 (the "LMI")
On the grounds of Article 64, paragraph 2, police authorities are entitled to issue mandatory orders (as a general rule written, unless it is impossible to do so and so long as they are understandable by the persons to whom the order is directed) if necessary to fulfil their functions. The orders must contain certain information determined by the law and are subject to appeal. Furthermore, in the process of detection, identification and deactivation of explosive devices and explosive substances, police authorities may block electronic communications by using technical means (Article 90).

Law on Gambling 2012
Web access may be blocked under a resolution of the State Commission on Gambling (the "Commission") if a violation of the gambling rules is not remedied within three days of a resolution setting out the violating websites. For the purposes of blocking the access, a request is then made by the State Commission on Gambling to the Chairman of the Sofia Regional Court and a writ of the court is published on the website of the Commission. The blocking of the web site is performed by the

relevant undertakings within 24 hours of the publication of the Court order at the web site of the Commission.

OVERSIGHT OF THE USE OF POWERS

Law on Special Intelligence Means 1999 (the "LSIM")
Control over the legitimate use of interception carried out under the LSIM is undertaken by the Head of the State Agency on Technical Operations if the special intelligence means are used by it; by the Head of the Technical Operations General Directorate with the State Agency on National Security, if the special intelligence means are used by the units of the agency; or by the Minister of Interior where special intelligence means are used in relation to the investigation involving undercover officer of the Ministry of Interior (Article 34a, para 2).

The monitoring of the procedures for authorization, enforcement and use of special intelligence means, the storage and destruction of information obtained through special intelligence means, as well as of protection of citizens' rights and freedoms against illegal use of special intelligence means is carried out by the National Special Intelligence Means Control Bureau (the "National Bureau") (an independent government agency, consisting of five people elected by the Parliament for five years and supported by an administrative office).

The National Bureau has the authority to request information from the state authorities that carry out functions related to special intelligence means (including interception), to issue mandatory instructions related to improvement of the regime of use and enforcement of special intelligence means, as well as of the storage and destruction of the information obtained through such means, and to citizens against which special intelligence means have been applied illegally. Where special intelligence means and storage and destruction of the data procured through use of these means have been used illegally, the National Bureau will notify the prosecutor's office and the heads of the controlling bodies and departments mentioned in the paragraph above.

Committee Oversight
Article 34h of the LSIM provides for a Committee for Oversight of the Security Services, the Deployment of Special Surveillance Techniques and the Access of Data under the Law on Electronic Communications. This is a Standing Committee constituted at the Bulgarian National Assembly under the Rules of Organization and Procedure of the National Assembly.

The Committee carries out parliamentary oversight and monitoring with respect to the procedures of authorization, enforcement and use of special intelligence means, the storage and disposal of data obtained, and the protection of civil rights and liberties against illegal use of special intelligent means, as well as the authorization of access and actual access to data under the LEC, and the protection of civil rights and liberties against illegal access to such data. Not later than 31 May of each year the Committee submits to the National Assembly a report on its activity which should contain summarized information on the issues mentioned above. In addition, the report should encompass any inspections and proposals made for improvements of the procedures of storage and processing of data under the LEC.

Please note that here is no explicit oversight in relation to special emergency powers. The Minister of Defence, however, does have oversight functions in the area of defence and carries out such functions through an inspectorate.

Law on Electronic Communications 2007 (the "LEC")
Under Article 261a of the LEC, the Personal Data Protection Commission (the "Commission") is the supervisory authority in relation to security of the data retained under Art. 251b, Paragraph 1.

The Commission has the right to require within its supervisory competence information from the undertakings which provide public electronic communications networks and/or services and issue binding instructions that are subject to immediate execution. In addition, each year the Commission provides the Bulgarian Parliament and the European Commission with summarized statistical information on:

(a) the cases in which retained data has been provided to the competent authorities;

(b) the time elapsed between the initial date on which the data has been retained and the date on which the competent authorities requested the provision of the retained data; and

(c) the cases where requests for retained data could not be executed.

Law on the Ministry of Interior 2006 (the "LMI")
The orders of the Minister of Interior for temporary restriction of certain activities may be appealed by the individuals or legal entities affected within seven days via the Minister of Interior before the Supreme Administrative Court (the "Court"). In this case the procedures under Administrative Procedure Code are followed.

In addition to the court procedures, the Administrative Procedure Code allows for individuals or organisations to contest administrative instruments before the superior administrative body (for example, the administrative procedure for contesting orders by the police, in relation to safeguarding human rights and civil liberties would be before the Director of Police, of officer that has issued the order). Appeal before the superior administrative body is not a prerequisite for further court appeal before the respective court.

PUBLICATION OF AGGREGATE DATA RELATING TO THE USE OF GOVERNMENT POWERS

Law on the Protection of Classified Information 2002 (the "LPCI")
Information relating to the lawful use of special intelligence means (including interception) is deemed to be a state secret as set out in Appendix 1 of the LPCI. Access to classified

information and state secrets is granted on a need-to-know basis to persons that have permission, and this permission may be granted by the State Commission for the Security of Information (Article 8) or the State Agency for National Security (Article 11). Therefore, publication of such information may not be published unless authorised by these agencies.

It should be noted that LPCI only affects information acquired using special intelligence means (including interception) and not, for example, requests for communications data retained under the Law of Electronic Communications.

Constitution of Bulgaria
Under Article 5, paragraph 5 of the Bulgarian Constitution, all laws must be published. Therefore, there is no power for the government to prevent anyone from publishing the laws to which they are subject.

Law stated as at 31 March 2015

DENMARK – 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 Danish law.

PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

Consolidation Act on Electronic Communications Networks and Services, 2014
(Act no. 128 of 7 February 2014, Bekendtgørelse af lov om elektroniske kommunikationsnet og –tjenester (the "Tele Act"))

The Tele Act, in conjunction with the Retention Order (described in section 2 below), sets out a telecom provider's obligation to make data available to the police, both by providing access to retained data and by providing interception capabilities.

According to section 10, a network operator or service provider must ensure that all technical equipment and systems used to provide an electronic communication network or service to end-users are set up in such a way that the police may intercept current communications and conduct mobile phone surveillance. In this context, mobile phone surveillance means the procurement of data that makes it possible to locate a mobile phone on a continuous basis as long as it is turned on.

Under section 10, the systems of the network operator or service provider must be set up to allow interception and immediate transmission of telecommunications data to another EU member state under the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 197/01).

In the case of a data interception request, the network operator or service provider must provide the IP-address, MAC-address or any similar identifier of the device making or receiving the communications that are to be intercepted.

Administration of Justice Act 2014 (Bekendtgørelse af lov om rettens pleje (Act no. 1308 of 12 December 2014, (the "AJA"))
Section 783 sets out the general rule that the police must obtain a court order and present it to the relevant network operator or service provider, before an interception may be made. The application for a court order must comply with the following conditions:

- there must be specific indications that communications, using the method of communication that is to be intercepted, are taking place to or from a suspect of the investigation;
- the interception must be decisive to the investigation; and
- the alleged offence must have a sentence of at least six years' imprisonment, or be one of a list of specified offences, such as desertion from the military or possession of child pornography.

In addition, interception must always be proportionate to the purpose for which it is to be used.

Section 783 (4) provides for an exception to the general rule. Where obtaining a court order would cause a delay that would defeat the purpose of carrying out the interception, the police may conduct the interception without obtaining a warrant first.

However when this happens, the police must, as soon as possible and no later than 24 hours from the interception, submit an application for a court order for the interception as set out above. The court then determines whether the interception was lawful, and if so, the length of time it should be allowed to continue. If the court finds that the interception was not lawful, it is obliged to notify the Ministry of Justice, which has statutory authority to investigate any breach of this process by the police.

Centre for Cybersecurity Act 2014 (Lov om Center for Cybersikkerhed (Act no. 713 of 25 June 2014, (the "Centre for Cybersecurity Act"))
The Danish Centre for Cybersecurity (the "Centre") has established a "net security service" (the "Service"), to which companies whose businesses have a socially important function, such as pharmaceutical companies, food companies and companies that administer administrative IT-systems, as well as most public institutions, can apply for connection. Through the Service, the Centre aims to discover, analyse and prevent cyber security breaches within the connected entities in order to maintain a high level of information security in Denmark, for example, to prevent hacking.

In order to connect to the Service, the relevant company or public institution must enter into an affiliation agreement with the Centre. Once connected, the Centre may process content and traffic data in the networks of connected entities to the Centre's Service, without obtaining a court order.

In addition to the entities described above, any company or public institution may temporarily connect to the Service if there is suspicion of a potential security incident based on specific and objectively identifiable facts, for example, if the company or institution has received threats from hackers.

At the time of writing this report, there are indications that new legislation in relation to the powers of the Centre for Cybersecurity Act may be introduced during 2015 but the precise nature of these new powers has not yet been formally announced.

DISCLOSURE OF COMMUNICATIONS DATA

Executive Order on the retention and storage of traffic data by providers of electronic communications networks and services
(No. 988 of 28 September 2006, as amended by executive order of amendment no. 660 of 19 June 2014 (Bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) (the "Retention Order"))

The Retention Order governs what data must be stored by a network operator or service provider.

Under section 5(1), a network operator or service provider must retain the following data about a user's access to the internet:

the allocated user identity (for example, the user name or customer number);

the telephone number which has been allocated to the user's communications as a part of a public electronic communication network;

the name and address of the subscriber or registered user to whom an IP address or user identity or telephone number had been allocated at the time of communication; and

the time of the beginning and the end of a communication.

Under section 5(2), a network operator or service provider providing wireless access to the internet must retain data concerning the local network's precise geographical or physical location, and the identity of the user's communication equipment. Data retained under the Retention Order must be stored for one year.

Consolidation Act on Electronic Communications Networks and Services 2014 (the "Tele Act")
According to section 10, a network operator or service provider must ensure that all technical equipment and systems used to provide an electronic communication network or service to end-users are set up in such a way that the police may obtain access to information about telecommunications traffic in the form of:

- telecommunications data, meaning information regarding which telephones or similar communications devices have been connected to a specific telephone or similar communications device either prior to or after the issue of an authorising court order; and
- extended telecommunications data, meaning information listing the connections made by the telephones or similar communication devices within a defined area (described by the police) either prior to or after the issue of an authorising court order (this would typically be information from cell phone masts);

Under section 13, when required by the police, network operators and service providers are obliged to disclose to the police data which identifies an end-user's access to electronic communications networks or services. This includes static information such as a designated IP-address, address, or phone number that the network operator or service provider has assigned to the end-user. The police can lawfully obtain this information without obtaining a court order.

A network operator or service provider which offers encrypted data as an integrated part of its service is obliged to decrypt an encrypted communication when complying with a court order. If, however, encryption has taken place outside of the services offered by the network operator or service provider, it will be the police's own responsibility to remove encryption from the provided data.

It is prohibited for network operators and service providers to retain content data. However, the police may retain, access and review the content of a person's correspondence, subject to the rules on lawful interception outlined in section 1 above.

Administration of Justice Act 2014 (the "AJA"))
The police may obtain access to historic telecommunications data in accordance with chapter 71 AJA. Section 783 sets out the general rule that, in order to do so, the police must obtain a court order and present it to the relevant network operator or service provider. The application for a court order must comply with the following conditions:

- there must be specific indications that communications are taking place to or from a suspect of the investigation using the method of communication that is to be intercepted;
- access to the relevant telecommunications data must be decisive to the investigation; and
- the alleged offence must have a sentence of at least six years' imprisonment, or be one of a list of specified offences, such as desertion from the military or possession of child pornography.

In addition, access to historic telecommunications data must be proportionate to the purpose for which it is to be obtained.

NATIONAL SECURITY AND EMERGENCY POWERS

Radio Frequencies Act (Act no. 475 of 12 June 2009, Lov om radiofrekvenser (the "RFA")), and the Order on maritime radio services in extraordinary situations (Executive order no. 916 of 13 November 2002, Bekendtgørelse om de maritime radiotjenester i ekstraordinære situationer (the "Maritime Radioservice Order")

According to section 32 RFA, and the Maritime Radioservice Order, the Danish Navy Operative Command may, in situations of crisis, war, catastrophes and other extraordinary situations, shut down the coastal radio station, and thus shut down normal public correspondence over coastal radio.

In accordance with section 33 RFA, the Danish Business Authority (the "DBA") (the regulatory supervisory authority for the telecoms industry under the remit of the Danish Ministry for Business and Growth) may prohibit the use of certain radio frequencies when the safety of the state demands it.

Under section 6 (5) RFA, the police, when exercising a power to disturb or interrupt radio and telecommunications that is granted under section 791(c) of the Administration of Justice Act, may do so without first obtaining a licence or other authorisation from the DBA to use the radio frequency spectrum in question.

CENSORSHIP

The Constitutional Act of the Kingdom of Denmark, 1953 (the "Constitution")
Under section 77 of the Constitution, censorship and other measures prohibiting freedom of expression are prohibited.

Gaming Act 2010 (Act no. 848 of 1 July 2010, Lov om spilth, (the "Gaming Act"))

As a general rule, government agencies do not have authority to block IP addresses, and the Telecommunications Industry Association (Teleindustrien) (a private industry organisation, of which the majority of Danish network operators and service providers are a part) has stated that network operators and service providers need only carry out DNS blocking following an authorising court order, and will not carry out any DNS blocking based solely on requests from intellectual property rights holders, government agencies or other third parties.

The only current exception to this is the Danish Gaming Board, which may request that a network operator or service provider blocks a website which contains illegal gambling systems.

OVERSIGHT OF THE USE OF POWERS

Judicial Oversight
Insofar as a court order is required to intercept or access retained data, or to block any website, the competent court will have oversight of this procedure.

Executive Order on the retention and storage of traffic data by providers of electronic communications networks and services (the "Retention Order")
The Retention Order was issued by the Danish Ministry of Justice (the "Ministry"). The Ministry oversees the compliance of network operators and service providers with the retention and storage requirements specified in the Retention Order. Non-compliance with the Retention Order may lead to financial penalties imposed by the Ministry.

Consolidation Act on Electronic Communications Networks and Services 2014 (the "Tele Act")
The Danish Business Authority (the "DBA") oversees compliance with the Tele Act by network operators and service providers. For example, it ensures that electronic communication networks are set up to enable interception by the police. Under chapter 33, section 79 of the Tele Act, both the DBA and the Telecommunications Complaints Board (the "Board") may enforce compliance and issue financial penalties for breaches of the Tele Act described in this report.

The Board comes under the remit of the Ministry for Business and Growth. Decisions taken by the DBA may be brought before the Board, and any decisions taken by the Board may be appealed to the High Court.

Administration of Justice Act 2014 (the "AJA"))
For the Danish police to conduct a lawful interception, section 783 of the AJA contains the general rule that they must first obtain a court order to do so. This rule is subject to certain exemptions which allow for an interception to take place without an order provided that the police make a submission to the court within 24 hours of the interception for its retrospective examination. If the court rules that the interception was not in compliance with law, it then notifies the Danish Ministry of Justice of the matter. The Ministry of Justice has statutory authority to investigate such non-compliance by the Danish police.

Centre for Cybersecurity Act 2014 (the "Centre for Cybersecurity Act")
For interceptions made in accordance with the Centre for Cybersecurity Act, the Centre for Cybersecurity (the "Centre") is solely responsible for determining whether to intercept. The Centre is placed under the Danish Security and Intelligence Service, within the Danish Ministry of Defence. In relation to the data processed by the Centre, the Danish Data Protection Act 2000 will not apply (nor does it apply generally to the police). However, the Minister of Justice and the Minister of Defence

appoints a supervisory board that supervises the Centre's use and processing of personal data.

Radio Frequencies Act 2009 and the Maritime Radioservice Order 2002
Under the RFA, the DBA determines whether consideration to the safety of the state demands the prohibition of the use of certain radio frequencies.

Under the Maritime Radioservice Order, the Danish Navy Operative Command determines whether the coastal radio station should be shut down.

Gaming Act 2010
The Danish Gaming Board oversees compliance by network operators and service providers with the Gaming Act.

PUBLICATION OF AGGREGATE DATA RELATING TO USE OF GOVERNMENT POWERS

Restrictions on network operators and service providers.
There are no restrictions on whether a network operator or service provider may publish aggregate data regarding government powers of interception, disclosure of communications data or censorship as described in this report. Equally, there are no restrictions on whether a network operator or service provider may publish descriptions or analysis regarding such powers.

Aggregate data published by government agencies.
Government agencies do not publish aggregate data in relation to their powers of interception, disclosure of communications data or censorship as described in this report.

Law stated as at 29 January 2015.

MALAYSIA – 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 Malaysian law.

PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

Legislation which specifically provides authority to intercept communications is summarised below. Where not explicit, these rights can be interpreted widely to require network operators and service providers to assist law enforcement and intelligence agencies in their surveillance and censorship activities.

Criminal Procedure Code (the "CPC")

Under section 116B, a police officer conducting a search under the CPC is to be given access to computerized data whether stored in a computer or otherwise. For the purpose of this section, "access" includes being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of the computerized data.

Section 116C gives the law enforcement and intelligence agencies very wide powers to intercept communications which may be evidence related to an offence.

Under section 116C, the Public Prosecutor (the Attorney General) may authorise a police officer to intercept any message transmitted or received by any communication, which may be evidence related to the commission of an offence. The CPC defines "offence" as any act or omission made punishable by any law for the time being in force, including offences such as money laundering or gambling. The Public Prosecutor may also require a communications service provider to intercept and retain a specified communication or communications of a specified description received or transmitted, or about to be received or transmitted by that communications service provider, or authorise a police officer to enter any premises and to install on such premises, any device for the interception and retention of a specified communication or communications of a specified description and to remove and retain such device.

Section 116C is silent as to whether a warrant is required, which will ultimately depend on the offence under investigation and the circumstances at hand. Under sections 62 and 116A, a search without warrant is possible if there is reasonable cause for suspecting that there is evidence of a security offence or organised crime concealed or any stolen property is concealed in any place and there are good grounds to believe that a delayed search is likely to result in their removal. A "security offence" has the same meaning as under the Security Offences (Special Measures) Act 2012 (set out immediately below).

Security Offences (Special Measures) Act 2012 (the "SOSM")

Section 6 SOSM allows the Public Prosecutor (the Attorney General) and police officers to intercept all communications likely to contain any information relating to the commission of a security offence. A "security offence" is an offence stated in chapter VI (offences against the state) or chapter VIA (offences relating to terrorism) of the Penal Code, for example, activity detrimental to parliamentary democracy, sabotage, waging war against the Yang di-Pertuan Agong (the King of Malaysia) and committing terrorist acts.

Section 6(1) states that the Public Prosecutor may authorise any police officer:

(a) to intercept, detain and open any postal article in the course of transmission by post;

(b) to intercept any message transmitted or received by any communication; or

(c) to intercept or listen to any conversation by any communication,

if he considers that it is likely to contain any information relating to the commission of a security offence.

Under section 6(2) SOSM, a police officer not below the rank of Superintendent of Police may do any of the above without authorisation of the Public Prosecutor in urgent and sudden cases where immediate action is required leaving no moment for deliberation. In practice, this may give police the power to intercept communications in a wide range of circumstances, including electronic communications.

Communications and Multimedia Act 1998 (the "CMA")
There are a wide range of offences provided for under the CMA, including breach of licence terms, and telecommunication specific issues such as improper or fraudulent use of network facilities/services.

Section 252 CMA authorises an authorised officer or a police officer of or above the rank of Superintendent to intercept communications if a public prosecutor believes a communication is likely to contain information relevant to an investigation into an offence under the CMA or its subsidiary legislation.

The CMA defines "authorised officer" as any public officer or officer appointed by the Malaysian Communications and Multimedia Commission (the "MCMC") and authorised in writing by the Minister with responsibility for communication and multimedia (presently the Minister of Communications and Multimedia (the "Minister")). "Intercept" is defined as the aural or other acquisition of the contents of any communications through the use of any electronic, mechanical, or other equipment, device or apparatus. "Communications" is defined as any communication, whether between persons and persons, things and things, or persons and things, in the form of sound, data, text, visual images, signals or any other form or any combination of those forms.

Furthermore, section 265 CMA gives the Minister the right to require implementation of interception capabilities by a licensee or class of licensees. A "licensee" is a person who either holds an individual licence, or undertakes activities which are subject to a class licence. There are four categories of licensable activities: Network Facilities Service Provider; Network Service Providers; Applications Service Provider; and Content Applications Service Provider. A telecommunications service provider must be licensed if it is providing licensable activities, and generally network service providers will be required to be licensed.

Please note that section 265 is silent as to whether the implementation of the interception capability would only be for purposes pursuant to a CMA offence. As a result, if read widely, it may cover offences outside of the CMA.

Section 38 gives the Minister the power to suspend or cancel an individual licence by declaration in certain circumstances, for example, if the licensee has failed to comply with the CMA or the conditions of its individual licence or the suspension or cancellation is in the public interest. Section 48 also provides similar cancellation powers to the Minister in respect of a class licensee.

Section 254 gives an authorised officer additional powers for the purposes of the execution of the CMA or its subsidiary legislation for specified purposes, including:

(a) to require the production of records, accounts, computerised data and documents kept by a licensee or other person and to inspect, examine and to download from them, make copies of them or take extracts from them; and

(b) to make such inquiry as may be necessary to ascertain whether the CMA or its subsidiary legislation have been complied with.

Copyright Act 1987 (the "Copyright Act")
Offences under the Copyright Act include making for sale or hiring any infringing copy, distributing infringing copies and circumvention of technological protection measures.

Under section 50B Copyright Act, the Public Prosecutor (the Attorney General) may authorise an Assistant Controller or a police officer not below the rank of Inspector Officer to intercept or to listen to any communications for the purpose of any investigation into an offence under the Copyright Act or its subsidiary legislation, if he considers that the communication is likely to contain information relevant to the investigation.

An Assistant Controller comes under the purview of the Intellectual Property Corporation of Malaysia (the "MYIPO"), and is appointed or deemed to be appointed by the Director General of the MYIPO under section 5 Copyright Act.

Section 43H Copyright Act provides a copyright owner whose right has been infringed to notify (in the manner determined by the Minister charged with the responsibility for intellectual property at the relevant time) a service provider to remove or disable access to the electronic copy on the service provider's network within 48 hours of receipt of notification.

Malaysian Anti-Corruption Commission Act 2009 (the "MACC")
Under section 43 MACC , if the Public Prosecutor (the Attorney General) or an officer of the Malaysian Anti-Corruption Commission (the "Commission") of the rank of Commissioner or above, as authorised by the Public Prosecutor, considers that it is likely to contain any information which is relevant for the purpose of an investigation into an offence under the MACC, it may authorise any officer of the Commission to intercept any message transmitted or received by any telecommunication, or to intercept, listen to and record any conversation by any telecommunication, and listen to the recording of the intercepted conversation.

Section 47 also imposes a legal obligation on every person to give information if required by an officer of the Commission or a police officer on any subject which it is such officer's duty to inquire into under the MACC.

Certain interception powers are also authorised to particular Law enforcement and intelligence agencies under the Kidnapping Act 1961, the Strategic Trade Act 2010, the Dangerous Drugs Act 1952, and the Dangerous Drugs (Forfeiture of Property) Act 1988.

DISCLOSURE OF COMMUNICATIONS DATA

As established above, various statutes provide wide powers of access, information gathering, search and seizure to law enforcement and intelligence agencies, which do not specifically distinguish between metadata and other types of data relating to communications, but may entail disclosure of such information. The following statutes give the relevant authorities wide powers of search and seizure that may include the right to access communications stored on a computer server.

Computer Crimes Act 1997 (the "CCA")
The CCA generally protects against the misuse of computers, for example, hacking. The CCA also provides wide powers of search, seizure and arrest to a police officer of or above the rank of Inspector. Under section 10, whenever there is reasonable cause to believe that in any premises there is evidence of the commission of an offence under the CCA, an officer may be empowered to enter the premises, by force if necessary, and there to search for, seize and detain any such evidence and he shall be entitled to:

(a) have access to any program or data held in any computer, or have access to, inspect or check the operation of, any computer and any associated apparatus or material which he has reasonable cause to suspect is or has been in use in connection with any offence under the CCA;

(b) require (i) the person by whom or on whose behalf the police officer has reasonable cause to suspect the computer is or has been so used; or (ii) any person having charge of or otherwise concerned with the operation of, the computer, apparatus or material, to provide him with such reasonable assistance as he may require; and

(c) require any information contained in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible.

Section 10(3) of the CCA also states that any police officer may arrest without a warrant any person whom he reasonably believes to have committed or to be committing an offence against the Act.

Anti-Money Laundering and Anti-Terrorism Financing Act 2001 (the "AMLATFA")
Section 31 AMLATFA confers wide powers on an investigating officer to conduct a search without a warrant if the officer is satisfied or has reason to suspect that a person has committed an offence under AMLATFA. These powers include searching for any property, record, report or document, and inspecting and taking possession of or making copies of or taking extracts from any record, report or document so seized and detained, and detaining them for such period as he deems necessary.

Section 37 requires any person to deliver any property, document or information which an investigating officer has reason to suspect:

(i) has been used in the commission of an offence under AMLATFA: or

(ii) is able to assist in the investigation of an offence under AMLATFA,

that is in the possession or custody of, or under the control of, that person or is within the power of that person to furnish.

Under section 67(1), similar powers exist where the competent authority or an enforcement agency has reason to believe that a person is committing, has committed or is about to commit an offence under AMLATFA.

The definition of "document" for these purposes is very wide and may be interpreted to include metadata relating to electronic communications.

Anti-Trafficking In Persons Act and Anti-Smuggling of Migrants Act 2007 (the "ATPAASMA")
Section 32 ATPAASMA stipulates that any enforcement officer conducting a search under ATPAASMA shall be given access to computerized data, whether stored in a computer or otherwise. For this purpose, the enforcement officer shall be provided with the necessary password, encryption code, decryption code, software or hardware or any other means required for his access to enable comprehension of the computerized data.

Communications and Multimedia Act 1998 (the "CMA")
The CMA gives the Malaysian Communications and Multimedia Commission (the "MCMC") information gathering powers. Section 73 gives the MCMC the right to direct any person to provide them with information if the MCMC has reason to believe that the person has any information or document relevant to the performance of MCMC's powers and functions or is capable of giving any evidence which MCMC has reason to believe is relevant to the performance of its powers and functions.

Under section 77, MCMC may take and retain, for as long as necessary, any document provided to it pursuant to its information-gathering powers.

Under section 247, a magistrate may issue a warrant authorising any police officer or authorised officer to enter premises if it appears to the magistrate that there is reasonable cause to believe an offence under the CMA or its subsidiary legislation is being or has been committed on the premises or that those premises contain any evidence or thing which is necessary to an investigation. The authorised officer may enter the premises at a reasonable time with or without assistance, and if need be by force, and to search for and seize any such evidence or thing. Section 247(8) states that if a search under section 247 indicates that there is any interference-causing equipment,

radio apparatus or radiosensitive equipment, the authorised officer may direct that necessary steps be taken to ensure an interference-free environment.

Section 249 CMA gives the police officer and authorised officer conducting a search under the CMA (whether with or without a warrant) access to computerised data, however stored. "Access" is defined to provide police with a full range of rights in relation to accessing data, including being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to comprehend computerised data.

Section 253 CMA makes it an offence to obstruct a search when a police officer or authorised officer is executing any duty imposed or conferred by law. If there is a court order or search warrant, the network operators and service providers may be liable for contempt of court if it refuses to assist.

General Consumer Code of Practice for the Communications and Multimedia. Industry (the "GCC")
The GCC requires a service provider to retain records of a customer's bill for a minimum period of one year. Material collected and recorded in relation to complaints handling processes is also to be retained by network operators and service providers for one year following the resolution of a complaint. However, the GCC also states that consumer data or information collected by service providers should not be kept longer than necessary.

The definition of "consumer" under GCC means a person who receives, acquires, uses or subscribes to services relating to communications and multimedia within the meaning of the CMA.

NATIONAL SECURITY AND EMERGENCY POWERS

Law enforcement and intelligence agencies have a number of special powers in times of emergency or for other special reasons. Below, we identify the common legislation invoked in such circumstances. Please note that there may be instances where emergency legislation is passed which is specific to a particular state within Malaysia. This is beyond the scope of this report.

Communications and Multimedia Act 1998 (the "CMA")
Under the CMA, a licensee shall, upon written request by the Malaysian Communications and Multimedia Commission (the "MCMC") or any other authority, assist MCMC or other authority as far as reasonably necessary in preventing the commission or attempted commission of an offence or otherwise in enforcing the laws, including the protection of the public revenue and preservation of national security.

Under section 266, on the occurrence of any public emergency or in the interest of public safety, the Yang di-Pertuan Agong (the King of Malaysia) or the authorised Minister may:

(a) suspend the licence of any licensee, take temporary control of any network facilities, network service, applications service and/or content applications service owned or provided by a licensee in any manner as he deems fit;

(b) withdraw either totally or partially the use of any network facilities, network service, applications service and/or content applications service from any licensee, person or the general public;

(c) order that any communication or class of communications to or from any licensee, person or the general public relating to any specified subject shall not be communicated or shall be intercepted or detained, or that any such communication or its records shall be disclosed to an authorised officer mentioned in the order; or

(d) order the taking of possession of any customer equipment.

Under section 266(c), on the occurrence of any public emergency or in the interest of public safety, the Yang di-Pertuan Agong or the authorised Minister may order that any communication or class of communications to or from any licensee, person or the general public relating to any specified subject shall not be communicated or shall be intercepted or detained, or that any such communication or its records shall be disclosed to an authorised officer mentioned in the order.

Emergency (Essential Powers) Act 1979 (the "EEPA")
Section 2 EEPA gives the Yang di-Pertuan Agong the power to make any regulations whatsoever (the "Essential Regulations") which he considers desirable or expedient for securing public safety, the defence of Malaysia, the maintenance public order and of supplies and services essential to the life of the community.

The Essential Regulations may, among other things, authorise the taking possession, control, forfeiture or disposition, on behalf of the Government of Malaysia, of any property or undertaking; or the acquisition, on behalf of the Government of Malaysia, of any property other than land; or authorise the entering and search of any premises; or provide for any other matter in respect of which it is in the opinion of the Yang di-Pertuan Agong desirable in the public interest that regulations should be made (sections 2(g), (h) and (o)).

Official Secrets Act 1972 (the "OSA")
Under section 6 OSA, any court may issue a search warrant to search for and seize a document, even though an offence under the OSA is not alleged, if it is satisfied that there is reasonable cause to believe a document contains matter or information prejudicial to the safety or interests of Malaysia and is directly or indirectly useful to a foreign power or to an enemy. "Document" is interpreted to include any other data embodied so as to be capable of being reproduced.

Section 12 OSA gives the Minister the power to require the production of certain messages sent to or from any place outside of Malaysia from any person who owns or controls any telecommunications device used for sending or receiving such messages (including the originals and transcripts of such messages and all other papers relating to the message). The request must be made by means of a warrant, and the

messages should be provided to the Minister or any person named in the warrant.

There is also a duty under section 11 OSA to provide information when required to do so by the police, by any member of the armed forces or by an authorised public officer.

Section 3(b) and (c) OSA stipulates that if, for any purpose prejudicial to the safety or interest of Malaysia, any person either makes any document or obtains, collects, records, publishes or communicates to another person any information which might be directly or indirectly useful to a foreign country, then they will be guilty of an offence punishable by life imprisonment. For the purpose of this section, "document" includes, in addition to a document in writing and part of a document:

(a) any map, plan, model, graph or drawing;

(b) any photograph;

(c) any disc, tape, sound track or other device in which sound or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom; and

(d) any film, negative, tape or other device in which one or more visual images are embodied so as to be capable (as aforesaid) of being reproduced therefrom.

Under section 27 OSA, in the course of any court proceedings related to an offence under the OSA, an application may be made for a court order by the prosecution to exclude the public from any part of a hearing. The grounds required are that the publication of any evidence or statements made in the course of the proceedings would be prejudicial to the safety of Malaysia.

CENSORSHIP

Communications and Multimedia Act 1998 (the "CMA")
In general, the Minister and the Malaysian Communications and Multimedia Commission (the "MCMC") are granted very wide powers to make determinations or declarations, the effect of which is that they may take control of or shut down network operators and service providers. Usually, the determinations or directives are issued pursuant to the CMA, which grants the Minister and the MCMC the power to issue determinations or directives on certain issues.

The CMA also contains several provisions regulating content and voluntary industry codes such as the Malaysian Communications and Multimedia Content Code (the "Code") (please see section 5.2 below) and General Consumer Code of Practice for the Communications and Multimedia Industry. Compliance with these voluntary industry codes by service providers is good practice but is not mandatory other than for licensed service providers and any person directed by the MCMC to comply. Failure to comply with such direction is an offence.

Section 211 of the CMA states that no content applications service provider shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person. Section 6 of the CMA defines content as any sound, text, still picture, moving picture, audio-visual or tactile representation, which can be manipulated, stored, retrieved or communicated electronically.

Under section 233, (a) a person who by means of any network facilities or network service or applications service knowingly makes, creates or solicits and initiates the transmission of obscene, indecent, false, menacing or offensive content with intent to annoy, abuse, threaten or harass any person; or (b) a person who knowingly by means of any network facilities or network service or applications service provides any obscene communication for commercial purposes or permits a network service or applications service under the person's control to be used for an activity described in (a), commits an offence.

Section 195 provides that the MCMC may use any of its powers under the CMA in the resolution of complaints received from consumers in relation to matters of customer service and consumer protection, including but not limited to, the failure of a licensee under the CMA to comply with a consumer code.

Malaysian Communications and Multimedia Content Code (the "Code")
The Code provides guidelines and procedures for good practice in relation to the dissemination of online content to the public by service providers in the communications and the multimedia industry. The Code also regulates Internet Content Hosting Providers ("ICH") and Internet Access Service Providers.

Companies who provide access to any electronic content (such as sounds, texts or pictures), but who do not control such content or have any knowledge of what it comprises, are deemed "innocent carriers". As such, they are not responsible for such content for the purposes of the Code.

The Code expressly states that ICHs are not required to do certain things, such as to block access by their users/subscribers to any material unless directed to do so by the Complaints Bureau, or monitor the activities of users and subscribers. (The Complaints Bureau is an arm of the Communications and Multimedia Consumer Forum, set up by the Malaysian Communications and Multimedia Commission to protect the rights of consumers in this sector. It deals with all complaints that relate to the Code.)

Anti-Money Laundering and Anti-Terrorism Financing Act 2001 (the "AMLATFA")
Section 6(3) stipulates that no person shall publish in writing or broadcast any information, including a report of any civil or criminal proceedings but excluding information published for statistical purposes by a competent authority or the Government, so as to reveal or suggest:

(a) that a disclosure was made under section 5; or

(b) the identity of any person as the person making the disclosure.

Section 5 relates to protection of informers and information relating to an offence under AMLATFA.

Sedition Act 1948

Section 10 states that the court may make an order prohibiting the issuing or circulation of a seditious publication which would be likely to lead to unlawful violence, or appears to have the object of promoting hostility between different classes or races of the community. The order will be given on the application of the Public Prosecutor (the Attorney General) and will require every person having any copy of the prohibited publication in his possession, power, or control to deliver every such copy into the custody of the police.

Bearing this in mind, some legal provisions may extend responsibility to network operators and service providers in relation to such laws even if the content is not actually provided or created by the network operators and service providers. These include abetting an offence punishable with imprisonment under section 116 of the Penal Code. In addition, under section 114A Evidence Act 1950, it is possible that the network operators and service providers may be presumed to be the publisher of the content contained on its customers' sites, unless the contrary is proved.

Other relevant legislation

In relation to enforcement measures, the Malaysian Communications and Multimedia Commission (the "MCMC") is authorised to block or remove scam websites or websites with illegal content and they largely work with the police and other enforcement agencies to implement this, for example, through use of the Penal Code and sedition laws. The Penal Code, for example, provides for offences in relation to complaints about violent "hate" sites, including section 505 which makes it an offence to make, publish or circulate any statement, rumour or report:

with intent to cause, or which is likely to cause, fear or alarm to the public, or to any section of the public whereby any person may be induced to commit an offence against the State or against the public tranquillity; or

with intent to incite or which is likely to incite any class or community of persons to commit any offence against any other class or community of persons.

The penalty for an offence under this section is up to two years' imprisonment, a fine, or both.

The Penal Code also contains offences in relation to printing content containing slander or libel, and offences in relation to hosted sites which contain illegal content or encourage illegal acts.

OVERSIGHT OF THE USE OF POWERS

Communications and Multimedia Act 1998 (the "CMA")
Under the CMA, section 18 states that the Appeal Tribunal established under section 17 may review any matter on appeal, from a decision or direction of the Malaysian Communications and Multimedia Commission (the "MCMC"), but not from a determination by the MCMC. Any decision by the Appeal Tribunal is final and binding on the parties to the appeal and is not subject to further appeal.

Section 120 provides that an aggrieved person or person whose interest is adversely affected by a decision or direction (but not a determination) of MCMC may appeal to the Appeal Tribunal for a review of the merits and the process of certain decisions or directions of the MCMC, unless the matter is not subject to an appeal to the Appeal Tribunal.

Section 121 provides for judicial review where a person is affected by a decision or other action of the Minister or Commission and all other remedies provided under the CMA have been exhausted.

Security Offences (Special Measures) (Interception of Communications) Regulations 2012 under the SOSM (the "2012 Regulations")
Regulation 3 requires that a police officer who has acted under section 6(3) SOSM (interception without authorisation by the Public Prosecutor in urgent cases where immediate action is necessary) must submit a written report to the Public Prosecutor (the Attorney General) containing specified information detailed in the Second Schedule of the 2012 Regulations. The information required includes details of the officer making the interception, details relating to the individual whose communication was intercepted, the facts surrounding the investigation and the grounds for using interception.

Anti-Money Laundering and Anti-Terrorism Financing Act 2001 (the "AMLATFA")
Section 31(4) requires the investigating officer, in the course of his investigation or search, to prepare and sign a list of all property, documents or information detained and state in the list the location in which or the person on whom, the property, document or information is found.

General power for Judicial Review ("JR")
Judicial review of the decision-making process of an authority exercising a power of a public nature by a court is available even if the executive/administrative decision is not open to any appeal or is expressed by the law to be 'final and conclusive'. Courts are not necessarily prevented from reviewing such acts or decisions.

The powers of the High Court in relation to JR are enshrined under the Specific Relief Act 1950 and the Courts of Judicature Act 1964. Grounds for JR include procedural impropriety, illegality, and irrationality in the decision-making process.

PUBLICATION OF AGGREGATE DATA RELATING TO USE OF GOVERNMENT POWERS

Restrictions on network operators and service providers
Under federal Malaysian law, there are no specific restrictions on publishing aggregate data relating to, for example, the volume of interceptions made in a single year. However, where not already set out in this report, the following laws could be employed to restrict such publication, in certain circumstances.

Communications and Multimedia Act 1998 (the "CMA")
The CMA provides confidentiality obligations in relation to evidence which is considered to be confidential by the Malaysian Communications and Multimedia Commission (the "MCMC") in the course of an investigation or trial (sections 24B, 61 and 63 CMA). Such confidentiality obligations are open to judicial review under section 121.

In addition, under section 80 CMA, the MCMC is itself bound by certain obligations in respect of the publication of information, and it may also issue a direction, requiring network operators or service providers to comply with similar obligations. Section 80(3) CMA states that the MCMC must not publish any information disclosed to it if the publication would:

(a) disclose a matter of a confidential character;

(b) be likely to prejudice the fair trial of a person; or

(c) involve the unreasonable disclosure of personal information about any individual (including a deceased person).

However, the MCMC may publish an abstract relating to such information provided that the particulars in the abstract are not be arranged in any way which would compromise or prejudice the person providing such information.

Aggregate data published by government agencies.

Anti-Money Laundering and Anti-Terrorism Financing Act 2001 (the "AMLATFA")
Section 6(3) AMLATFA (described in section 4.3 above) prevents the disclosure of certain information in legal proceedings, however, it exempts information published for statistical purposes by a competent authority or the government.

Generally, however, government agencies do not publish aggregate data in relation to the federal powers of interception, disclosure of data or censorship, as described in this report.

Law stated as at 15 January 2015.

MONTENEGRO – 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 Montenegrin law.

PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

Constitution of Montenegro (Official Gazette of Montenegro no.1/2007 and 38/2013, Ustav Crne Gore) (the "Constitution")
The Constitution guarantees confidentiality of letters, telephone conversations and other means of communication and provides that derogation from this right is allowed only on the basis of a court decision if necessary in criminal proceedings or for national security(Article 42).These rights may only be limited by the law, for the purpose provided by the Constitution and to the extent necessary to satisfy the constitutional purpose of the limitation in question in an open and free democratic society (Article 24).

Electronic Communications Act (Official Gazette of the Republic of Montenegro nos. 40/2013 and 56/2013, Zakon o elektronskim komunikacijama) (the"ECA")
The ECA prohibits interception of electronic communications unless it is necessary, adequate and proportionate in the interests of national security, defence, prevention of crime, investigation of a crime, revealing and prosecuting criminal offenders or combatting the unauthorised use of a system for electronic communications, as well as for finding or rescuing people and for the protection of lives and property (Article 172, paragraphs 2 and 4).

In relation to the powers available under Article 172, network operators and service providers are obliged to provide, upon the request of the competent government agency, and at their own expense, necessary technical and organizational conditions to enable interception of communications, and to inform the Agency for Electronic Communication (the "Agency") about the interception. Network operators and service providers are obliged, in cooperation with the government agency on whose request the interception is performed, to make a permanent record of the fact that the communication was intercepted and to keep any data collected, and the fact that the data has been collected in such a way, a secret (Article 180).

The ECA does not impose an obligation on network operators and service providers to directly intercept individual customer communications, nor does it specify which government agencies are authorised to request interception. The ECA does not provide a maximum duration for an interception. Since such interception is allowed by the Constitution for the purpose of conducting criminal proceedings or for the protection of national security, however, only the competent criminal court (whose order is implemented by the police) and the Agency for National Security (the "ANS") are authorised to require such interception under the conditions stipulated in the ECA and the legislation concerning their activities. The maximum duration for each interception is regulated by the specific legislation applicable to the activities of criminal courts and the ANS.

Criminal Procedure Code (Official Gazette of Montenegro nos. 57/2009, 49/2010 and 47/2014, Zakonik o krivičnom postupku) (the"CPC")
Under the CPC, interception and surveillance of electronic communications are stated to be secret surveillance measures available both at the pre-investigation stage and the investigation stage of criminal proceedings. Such measures may be ordered against a person suspected of committing or preparing certain categories of crimes, if evidence of that crime cannot be collected in any other way, or if gathering of evidence by other means would cause disproportional risk or jeopardize lives (Article 157). The relevant crimes for this purpose are those punishable with imprisonment of 10 years or more, organized crime, and certain crimes with elements of corruption, such as money laundering, cyber-crime and blackmail (Article 158).

Interception may also be ordered against a person who is under

reasonable suspicion of transferring messages to and from a suspect related to one of these crimes, or whose phone or other means of communication are used by a suspect (Article 157). The order for such interception is issued by the competent criminal court, upon the written request of the State Prosecutor for a maximum period of four months, with the possibility of an extension of three months (Article 159). The court's order must be accompanied with a separate order containing the phone number or email address of the suspect to be intercepted and the duration of the interception, which will be implemented by the police, to whom the network operator or service provider shall provide all necessary assistance (Articles 159 & 160).

Exceptionally, if written approval cannot be issued in time, and delay would be detrimental to the investigation, interception may commence based on the oral approval of the investigation judge, in which case written order for interception must be issued within 12 hours of obtaining oral approval (Article 159). Network operators and service providers are obliged to enable the interception of communications by authorised police (Article 159 and Article 160). If the State Prosecutor decides not to initiate criminal proceedings against the suspect, the collected materials must be delivered to the investigation judge for destruction (Article 160). Evidence collected by interception which was not ordered or performed in accordance with this procedure will be declared inadmissible and the competent court shall order their destruction (Article 161).

The Agency for National Security Act (Official Gazette of Montenegro, nos. 28/2005, 86/2009, 73-2010 and 20/2011, Zakon o Agenciji za nacionalnu bezbjednost) (the "ANSA")

ANSA authorises the ANS to collect data by secret interception and surveillance of electronic communications if other investigation measures would not provide an adequate result, or if it would cause disproportionate risk or threaten lives or health (Article 9 and 13).

When there is a reasonable suspicion of a threat to national security, an interception may be ordered by a decision of the President of the Supreme Court of Montenegro, or in his/her absence the designated judge of that court (Article 14).

Such interception is ordered for a period of three months, and for serious reasons may be extended in additional three month periods, but its overall duration must not exceed 24 months (Article 15). Article 15 also provides that network operators and service providers are obliged to enable and guarantee conditions necessary for such interception.

DISCLOSURE OF COMMUNICATIONS DATA

Electronic Communications Act (Official Gazette of Montenegro nos. 40/2013 and 56/2013, Zakon o elektronskim komunikacijama) (the "ECA")

Network operators and service providers are obliged to retain certain data on traffic and location, as well as data relevant for identification and registration of their customers. Such data may only be retained for the purposes of national security, defence, prevention of crime, investigation, revealing and prosecuting criminal offenders or the unauthorised use of a system for electronic communications. It may also be used to find or rescue people and for the protection of lives and property (Article 181 ECA).

Network operators and service providers must also provide, at their own expense, necessary technical and organizational conditions which would enable competent government agencies to take over such data (Article 181). This would oblige a network operator or service provider to decrypt encrypted data when required to do so by court order.

The period of retention must not be shorter than six months nor longer than two years from the moment the communication occurred (Article 181, paragraph 5).Government agencies may request access to the metadata retained by network operators and service providers. Network operators and service providers are obliged to keep annual records and statistics on data which have been delivered to government agencies and records on requests for delivery of retained metadata which could not be executed (Article 181, paragraph 6).

According to Article 182, network operators and service providers are obliged to retain data on:

(a) tracing and identifying the source and destination of a communication;

(b) identifying the location of the parties to the communication;

(c) determining date, time and duration of a communication;

(d) identifying the type of communication;

(e) identifying users' terminal equipment; and

(f) identifying the location of the users' mobile terminal equipment.

Under the provisions of Article 181, paragraph 3, network operators and service providers must not retain the content of customer communications. However, since Article 180, paragraph 2 allows interception of electronic communications on the basis of a court decision, if such court decision contains an order for the retention of the content of electronic communications, network operators and service providers would be obliged to act upon it.

Article 183, paragraph 1, obliges network operators and service providers to ensure that the quality and level of protection of retained metadata is the same as the quality and level of protection of the data circulating on the network. In addition, operators should undertake adequate technical and organizational measures to prevent unlawful or accidental destruction, loss or modification of retained metadata, unauthorised storage, processing, access or disclosure of the retained metadata. Access to the retained metadata should only be granted to those persons authorised by the network operator or service provider. Any metadata not accessed at

the end of a prescribed period of retention must be destroyed.

Criminal Procedure Code (Official Gazette of Montenegro nos. 57/2009, 49/2010, 47/2014 , Zakonik o krivičnom postupku) (the "CPC")
Under the CPC, if there is a reasonable suspicion that a prosecutable offence has been committed, the police may, by their own volition, or at the request of the State Prosecutor, inform the Public Prosecutor of all necessary actions required to collect information which would be useful for criminal prosecution, including requesting network operators and service providers to disclose the metadata of a particular communication (Article 257). However, in its decision U-I 34/2011 of July 23, 2014 the Constitutional Court of Montenegro declared unconstitutional the part of Article 257 that allowed the police to request metadata from network operators and service providers without a court decision. Network operators and service providers are, therefore, obliged to disclose retained metadata only on the basis of a court decision.

Police Act (Official Gazette of Montenegro nos. 44/2012, 36/2013 and 1/2015, Zakon o unutrašnjim poslovima) (the "PA")
Under the PA, the police are authorized to collect personal and other data to the extent necessary for performance of their activities aimed at prevention and suppression of crimes and protection of public order (Article 37 of PA). State bodies, local authorities and legal entities are obliged to enable inspection and to deliver, at the request of the police, data from their records.

The request made by the police to collect the data must contain the folllowing:

(a) the legal grounds for the collection of the data;

(b) the details of the requested data;

(c) the purpose for which the data are requested;

(d) sufficient information necessary for determining the identity of a person to whom the requested data are related; and

(e) a warning that it is a criminal offence to reveal to any third party the content of the request or which data is provided under it.

The police may also electronically inspect the records kept by legal entities if the entity has the technical arrangements to allow electronic inspection.

However, if the data requested is:

(f) for the purpose of commencing or continuing a criminal investigation, the police are not obliged to state in the written request why the criminal investigation is starting or continuing; and

(g) based on a court`s order or state prosecutor`s order, the police do not have to explain why the data is being requested (Article 39 of PA).

The Agency for National Security Act (Official Gazette of Montenegro, nos. 28/2005, 86/2009, 73/2010 and 20/2011, Zakon o Agenciji za nacionalnu bezbjednost) (the "ANSA")
On the written request of the ANS, network operators and service providers are required to enable access to data contained in their records and to keep all such requests a secret (Article 8). On the basis of a court decision, the ANS is authorised to collect data by secret interception and surveillance of electronic communications if other investigation measures would not provide an adequate result, or if it would cause a disproportionate risk or threaten people's lives or health (Article 9 and 13).

ANSA does not contain a definition of surveillance and therefore it is not clear whether collection of metadata from network operators and service providers falls within Article 8 or Article 9. However, decision U-I 34/2011 of July 23, 2014 of the Constitutional Court of Montenegro states that the collection of metadata for the purpose of conducting criminal proceedings is allowed only on the basis of a court order.

Furthermore, the Agency for Personal Data Protection (the "Agency for PDP"), which monitors data protection and is authorised to issue opinions concerning the interpretation of laws related to data protection, rendered two opinions concerning the obligation of network operators and service providers to disclose metadata to government agencies (opinion no. 993/2014 of February 11, 2014 and opinion no. 5342/2014 of July 23, 2014).

These opinions, are not binding, but indicate the position of the Agency for PDP, namely that network operators and service providers are obliged to disclose the retained metadata to the police and the ANS only on the basis of a court order, if data are required for the purpose of national security, defence, prevention of crime, investigation, revealing and prosecuting of criminal offenders or unauthorised use of a system for electronic communications. However, the Agency for PDP holds that in cases of police activity related to finding or rescuing people which are not conducted for the purpose of criminal investigation or prosecution, network operators and service providers may, even without a court order, disclose the retained metadata to the police.

NATIONAL SECURITY AND EMERGENCY POWERS

Defence Act (Official Gazette of Montenegro, nos. 47/2007, 86/2009, 88/2009, 25/2010, 40/2011 and 14/2012), Zakon o odbrani) ("DA")
In a "state of emergency", defined as natural disasters, technology or environmental disasters, epidemics, danger to the public security or threat to the constitutional order (Article 5, paragraph 1, subparagraph 6) or "state of war", defined as the state of imminent war, danger or military attack on the territory of Montenegro (Article 5, paragraph 1, subparagraph

7), legal entities in the field of postal-telegraph-telephone traffic and other carriers of telecommunications systems must prioritise the delivery of services as specified by the Ministry of Defence (Article 21, paragraph 1).

Electronic Communications Act (Official Gazette of Montenegro nos. 40/2013 and 56/2013, Zakon o elektronskim komunikacijama) (the "ECA")
The ECA obliges network operators and service providers to prepare an action plan for protection of the integrity of electronic communications networks and their usage in a state of emergency or war and to submit it to the Ministry of Information Society and Telecommunications, the Agency for Electronic Communications, and other competent state bodies in charge of defence and security (Article 61, paragraphs 1 and 3).

Network operators and service providers are obliged to make available their electronic communications networks to the competent state bodies (Article 61, paragraph 4) and to provide prioritised communication between certain terminal points which are defined by the government. For the purpose of enabling such prioritised communication, the government may order a network operator or service provider to temporarily disable its other network connections or to undertake other measures, if it deems it necessary (Article 62).

Constitution of Montenegro (Official Gazette of Montenegro no.1/2007 and 78/2013, Ustav Crne Gore) (the "Constitution")
In a state of emergency or a state of war the Constitution allows the introduction of measures which derogate from the overarching principle of confidentiality of letters, telephone conversations and other means of communication and protection of personal data (Article 25).Consequently, in such instances government agencies may request access to customer communications data and/or their networks held by network operators and service providers, without following the usual procedure of presenting a court decision authorising interception or access to retained data. According to Article 132 and 133, a state of war or emergency is proclaimed by the Parliament, or by the Council for the Security and Defence if the Parliament is not in position to convene.

CENSORSHIP

Enforcement and Security Act (Official Gazette of Montenegro, no. 36/2011 and 28/2014, Zakon o izvršenju i obezbeđenju) ("ESA")
Although there is no specific provision which explicitly regulates censorship or the blocking of IP addresses, network operators and service providers would be obliged to censor customer communications pursuant to the ESA, if such an order were given by a competent court in the form of an interim measure on the basis of some other law or in the form of a final court decision.

OVERSIGHT OF THE USE OF POWERS

Judicial Oversight
Since the CPC and ANSA provide that interception of electronic communications is allowed on the basis of a court order, each interception is overseen by the competent criminal court which ordered the interception and which monitors its enforcement (Article 180, paragraph 2 ECA; Article 159, paragraphs 1 and 5 and Article 160 CPC; Articles 14 and 15 ANSA).

Electronic Communications Act (Official Gazette of Montenegro nos. 40/2013 and 56/2013, Zakon o elektronskim komunikacijama) (the "ECA")
Although the ECA does not explicitly mention oversight of the interception procedure, it contains provisions concerning the general oversight of network operators and service providers operations conferred to the Agency for Electronic Communications (the "Agency") and to the Administrative state body for inspection tasks (Articles 184 and185). According to Article 189, paragraph 1, subparagraph 6, the Agency monitors the security of an operator's or a service provider's electronic communications network and services and their compliance with the provisions relating to the confidentiality of communications. The Agency is authorised to order network operators and service providers to undertake, within a reasonable deadline, measures necessary for adjusting their activities in line with the statutory requirements to keep communications confidential (Article 189, paragraph 3).

Article 180, paragraph 1, obliges network operators and service providers to inform the Agency about their technical and organizational capabilities which enable interception of electronic communications. The Agency monitors the work of network operators and service providers and is authorised to request a network operator or service provider to correct any irregularity in its technical and organizational settings (Articles 188 and 189).

According to Article 183, paragraph 2, control over the measures taken by network operators and service providers for the purpose of ensuring security of retained metadata is performed by the Agency for Personal Data Protection (the "Agency for PDP"). The Agency for PDP is authorised to request information from both network operators and service providers and government agencies performing the interception in relation to the collection and protection of personal data of customers. If data is not processed in accordance with the law, the Agency for PDP may order one of the following measures: the rectification of irregularities within a specified period of time; a temporary ban on any data processing carried out contrary to the provisions of the law; and the deletion of personal data collected without proper legal grounds (Article 71 Personal Data Protection Act (Official Gazette of Montenegro nos. 79/2008, 70/2009, & 44/2012, Zakon o zaštiti podataka o ličnosti)).

Police Act (Official Gazette of Montenegro nos. 44/2012, 36/2013 and 1/2015, Zakon o unutrašnjim poslovima) (the "PA")
According to Articles 114, 115 and 119 PA, police activities are

generally supervised by a special department of the Ministry of Police for Internal Control, which monitors the legality of police work, especially with regards to respect and protection of human rights in the performance of police tasks and applying police powers, and delivers its reports to the Minister of Police and the government at least once per year.

Police activities are also generally monitored by the Council for Civil Control, a special body comprised of members of the Bar Association, Doctors Association, Lawyers Association, University of Montenegro and nongovernmental human rights organizations, which evaluates police work and provides recommendations for improvement of their activities to the Minister of Police (Article 112 & 113).

The Agency for National Security Act (Official Gazette of Montenegro, nos. 28/2005, 86/2009 and 20/2011, Zakon o Agenciji za nacionalnu bezbjednost) (the "ANSA")
The work of the ANS is monitored by the Chief Inspector appointed by the Government (the role of which is outlined above) (Article 40). Political supervision over the work of the police and the ANS is conferred to parliament (Article 110 and 111 PA and Article 43 ANSA).

Law on Constitutional Court of Montenegro (Official Gazette of Montenegro, no.64/2008, 46/2013 and 51/2013 Zakon o ustavnom sudu Crne Gore)
Network operators and service providers may also file a constitutional appeal against an individual decision of a government agency which violates the constitutional guarantees, when other legal remedies, such as complaints or appeal procedures with the relevant agency or court, have been exhausted or are not prescribed or where the right to their judicial protection has been excluded by law (Articles 48 and 49).

Constitution of Montenegro (Official Gazette of Montenegro no.1/2007 and 38/2013, Ustav Crne Gore) (the "Constitution")
According to Articles 132 and 133, all measures which would provide for derogation from confidentiality of letters, telephone conversations and other means of communication and protection of personal data, which would be adopted by the Council for the Security and Defence, must be ratified by the Parliament when in a position to convene.

Furthermore, the Constitutional Court of Montenegro, which is authorised to assess constitutionality and legality of laws and other general acts, may find that a measure of derogation introduced during a state of war or a state of emergency is unconstitutional (Article 149).

PUBLICATION OF AGGREGATE DATA ON THE USE OF GOVERNMENT POWERS

There is no law prohibiting the publication of any of the laws mentioned in this report or any description of the powers set out in those laws.

Electronic Communications Act (Official Gazette of the Republic of Montenegro nos. 40/2013 and 56/2013, Zakon o elektronskim komunikacijama) (the"ECA") and
Under article 30, paragraph 1 of the ECA, network operators and service providers must deliver to the Agency for Electronic Communications all available data concerning the development of the electronic communications network or the services provided, with the exception of data relating to intercepted communications and disclosure of metadata. Furthermore, article 180, paragraph 3 of the ECA requires network operators and service providers to make a permanent record of all interceptions in collaboration with the government agency that requested the interception. These records must be kept secret.

This indicates that the records of interception activities and requests for provision of metadata by the police and other government agencies (except for the Agency of National Security, see paragraph 33.2 below) may not be published by network operators or service providers. However, there is no law to prevent the publication of aggregate data (i.e. the number) relating to these requests.

The Agency for National Security Act (Official Gazette of Montenegro, nos. 28/2005, 86/2009 and 20/2011, Zakon o Agenciji za nacionalnu bezbjednost) (the "ANSA")
Article 8 of the ANSA provides that network operators and service providers must keep secret all details relating to all requests received by the Agency of National Security. Aggregate data relating to these requests, therefore, may not be published.

Law stated as at 20 January 2015.

MYANMAR – 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 Myanmar law.

PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

Telecommunications Law No.31/2013 (the "2013 Law")
The 2013 Law was drafted to update Myanmar's telecommunications sector and to provide a legal framework for the introduction of foreign private investment in the industry. It repealed the Myanmar Telegraph Act 1895 (the "1895 Act") and the Myanmar Wireless Telegraph Act 1934, although under section 85(b) of the 2013 Law, rules, notifications, orders and directives issued under the older legislation may continue to be applicable insofar as they are not inconsistent with the new law. There are also additional rules and regulations in relation to the 2013 Law, which are at varying stages of coming into force. The first of these are the Licensing Rules, which were introduced by Notification No. 16/2014 on 14 October 2014 (the "Notification").

Under section 75 of the 2013 Law, the government may as necessary direct the relevant organisations to intercept any information or communications that may adversely affect national security or the rule of law and order, so long as the exercise of such powers does not infringe the fundamental rights of the citizens (as set out in the 2008 Constitution of Myanmar).

In general, all service providers wishing to provide network, network facility or application services must be licenced (section 5 of the 2013 Law) and so will be licence holders. Under section 77, the Ministry of Communications and Information Technology (the "MCIT") has wide discretion to direct a licence holder to intercept communications, when it is in the public interest and with the approval of the government. The 2013 Law does not contain a test to determine what constitutes "in the public interest".

Section 5(1) of the 1895 Act, however, authorises the President of the Union or an authorised representative, in times of public emergency or in the interests of public safety, to take temporary possession of, block, detain, intercept or disclose any telegraph, which may indicate how "in the public interest" would be interpreted under section 77 of the 2013 Law.

Section 5(2) of the 1895 Act states that if any doubt arises as to the existence of a public emergency, or whether any act done under section 5 (1) was in the interest of the public safety, a certificate signed by a Secretary to the Government is conclusive proof on the point.

In relation to monitoring and enforcement of licences, section 36(a) (ii) of the Notification also refers to a lawful interception request in the context of when a licensee may be exempt from providing certain information to the Telecommunications Department of the MCIT. There is currently no clarification as to what constitutes a lawful interception request.

Section 78 of the 2013 Law provides that a licensee must make necessary preparations to enable a telecommunication service to be utilised for security matters in accordance with the law. This suggests that a telecommunications provider may be required to assist the government in the implementation of interception capabilities on its network.

DISCLOSURE OF COMMUNICATIONS DATA

Telecommunications Law 2013 (the "2013 Law")
Under section 17 of the 2013 Law, a licensee must keep information transmitted or received through its telecommunications service confidential and must not disclose the confidential information of each user to any unauthorised or irrelevant person except for matters allowed by the existing laws (such as those set out in sections 75 to 78, described above).

There is no definition of "irrelevant party" but this may be interpreted to mean any unauthorised third party. Section 36 of the Notification, however, provides that, the Telecommunications Department of the Ministry of Communications and Information Technology (the "Department") may:

(a) establish regular, reasonable reporting requirements on the activities of all or certain categories of Licensees; and

(b) issue a written request to specific licensees for any information, data, document, agreement, operating log, papers or other information required by the Department to discharge its functions under the 2013 Law, provided that such request is reasonable, not unduly burdensome and affords the licensee at least thirty days to provide the requested information unless subject to a lawful interception request.

Under section 36(b) of the Notification, licensees are obliged to comply with this request.

In addition, section 38 of the Notification states that the Department has the authority to inspect the facilities and documents of any licensee, subject to a reasonable notice period prior to inspection and provided that the inspection has a legitimate aim and is proportionate and necessary for the purpose for which inspection is undertaken.

The wording of sections 17 and 69 of the 2013 Law also implies that disclosure may be required in the context of legal proceedings and under a court order. Section 69 of the 2013 Law makes it an offence to disclose any information which is kept under a secured or encrypted system unless in the context of court proceedings relating to telecommunications and when ordered to disclose such information by the court.

Furthermore, section 95 of the Code of Criminal Procedure 1898 (the "Code") states that only a District magistrate, High Court or Court of session may require the delivery to any person they direct of "any document, parcel or thing" that is in the custody of the postal or telegraph authorities in relation to an investigation, inquiry, trial or any other proceeding under the Code.

NATIONAL SECURITY AND EMERGENCY POWERS

Telecommunications Law 2013 (the "2013 Law")
Under section 76, the Ministry of Communications and Information Technology (the "MCIT") or the department or organisation assigned by it may, for defence and security matters of the State or for the public interest, enter into and inspect, supervise and require submission to it of any documents relating to the service activities of the telecommunications service provider. "Service activities" is not defined and there is no detail provided in the law regarding how this section would be implemented. Note, however, that a licensee's permitted activities will also be contained in its individual licence.

CENSORSHIP

Telecommunications Law 2013 (the "2013 Law")
Section 77 of the 2013 Law permits the Ministry of Communications and Information Technology (the "MCIT") to restrict and block certain kinds of communications and to control and use the business of any telecommunications service provider and its telecommunications devices when it is deemed in the public interest and with the approval of the government. The method by which this provision would be enforced is unclear. Under section 22 of the Notification the Telecommunications Department of the MCIT (the "Department") is given authority to direct the Licensee to suspend any services rendered pursuant to a licence or to terminate a licence, either following a breach of the terms and conditions of a licence by the licensee, or failure by the licensee to comply with the duties of a licensee or with any directives or resolutions issued by the MCIT or the Department.

Electronic Transactions Law 2004 (the "ETL")
The ETL applies to any kind of electronic record and electronic data message used in the context of commercial and non-commercial activities. Section 33 makes it an offence to undertake any act by using electronic transactions technology which is detrimental to the security of the State or prevalence of law and order or community peace and tranquillity or national solidarity or national economy or national culture. This may be interpreted widely.

The method by which this provision may be enforced is unclear.

OVERSIGHT OF THE USE OF POWERS

The Constition of the Republic of the Union of Myanmar (2008) (the "2008 Constitution")
The 2008 Constitution includes the grant of certain fundamental rights, including of freedom of expression, to each citizen so long as such rights are not exercised in a way that is contrary to laws that are enacted for the security of the state, the prevalance of law and order, community peace and tranquility or public order or morality. The Constitution also requires the government to protect the privacy and security of correspondence and other communications under the law, subject to its other provisions.

Telecommunications Law 2013 (the "2013 Law")
As a general comment, one of the overarching objectives of the 2013 Law is to provide legal protection to both telecommunication service providers and to the users of such services.

The Ministry of Communications and Information Technology (the "MCIT") must seek government approval to request an interception under section 75 of the 2013 Law or to block or restrict access to communications under section 77. There is no clarification of what form government approval would take (for example, as an executive order or parliamentary resolution).

However, under section 82, in matters of national emergency, natural disaster or for national defence and security, the

MCIT may exempt any government department, organisation or person from obtaining any permission, licence or recommendation required under the law without the prior approval of the government. Such exemptions must, however, be submitted to the government.

Judicial Oversight
There is no specific judicial oversight process laid out in law. Where disclosure of data is required in the context of legal proceedings, the competent court may control such disclosure.

PUBLICATION OF AGGREGATE DATA RELATING TO USE OF GOVERNMENT POWERS

There is no law in Myanmar preventing the publication of aggregate data relating to the use of the powers described above. Furthermore, no law prevents the publication of laws which set out the powers of government agencies or descriptions of those powers.

Law stated as at 27 January 2015.

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.

PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

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 1902 (the "Penal Code") 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.

The police may be empowered to conduct an interception itself, 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 unit, investigation unit, surveillance unit and the technology unit.

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, then 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).

Police Act 1995 (Lov om politiet (LOV-1995-08-04-53)) (the "PA")
According to section 17d PA, the district court may 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.

DISCLOSURE OF COMMUNICATIONS DATA

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 has 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 placement 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.

Electronic Communications Act (Act No. 83 of 04 July 2003) (the "ECA")
Section 2-7 ECA regulates 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.

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, 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.

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 17 d of the Police Act, the provisions set out below may provide government agencies with further powers in relation to national security and emergencies.

General Civil Penal Code 1902 (the "Penal Code")
According to section 47 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 48 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 dangerousness of the attack, the guilt of the assailant or the legal right that is threatened by the attack.

Provided that the conditions in section 48 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.

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.

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. At the time of writing this report, no further developments had taken place.

CENSORSHIP

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.

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.

OVERSIGHT OF THE USE OF POWERS

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 12 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.

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.

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.

Law stated as at 21 January 2015.

SERBIA – 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 Serbian law.

PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

Constitution of the Republic of Serbia (Official Gazette of the Republic of Serbia no. 98/2006, Ustav Republike Srbije) (the "Constitution")
The Constitution guarantees the confidentiality of letters and other means of communication, and provides that derogation from this right is allowed only if necessary to conduct criminal proceedings or to protect the security of the Republic of Serbia, in a manner stipulated by the law and by a decision of a competent court. Any such derogation must be for a specified period of time (Article 41).

Electronic Communications Act (Official Gazette of the Republic of Serbia nos. 44/2010, 60/2013 and 62/2014, Zakon o elektronskim komunikacijama) (the "ECA")
The ECA obliges network operators and service providers to enable lawful interception of electronic communications required by government agencies for the purpose of criminal investigations (Article 37, paragraph 2, subparagraph 17 and Article 127, paragraph 1). Interceptions of electronic communications which reveal the content of a communication are allowed only for a limited period of time and on the basis of a court decision, if such interception is necessary to conduct criminal proceedings or for the protection of national security (Article 126, paragraph 1).

The ECA does not specify which government agencies may request interception, or the maximum duration of an interception. However, since interception is allowed for the purpose of conducting criminal proceedings or for the protection of national security, only government agencies which operate in these areas (the police, the State Prosecutor, the Security-Intelligence Agency and the Military Security Agency) would be authorised to require interception in accordance with the ECA and the legislation specific to their activities (described further below), which also regulate the maximum duration of each interception.

Article 37 and Article 127 provide that network operators and service providers have an obligation to enable lawful interception of electronic communications. Article 127 obliges network operators and service providers to provide, at their own expense, the necessary technical and organizational setting (equipment and software support) to enable interception of electronic communications that reveal the content of communications and to inform the Agency for Electronic Communications (the "Agency") about the interception. The interception of electronic communications must be authorised by a decision of the competent court, which will specify the government agency designated to conduct the interception.

According to the ECA, if a government agency is authorised to intercept an electronic communication and is able to do so without requiring assistance to access the premises, the electronic communications network, other instruments or the electronic communications equipment of the network operator or service provider, the obligation to keep records of the interception lies with the government agency conducting the interception (Article 127, paragraph 2). Conversely, if the government agency is not able to conduct the interception without assistance, these records must be kept by the network operator or service provider (Article 127, paragraph 3). In both instances, a court decision is required to authorise the interception (Article 126, paragraph 1).

Criminal Procedure Code (Official Gazette of the Republic of Serbia nos. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 and 55/2014, Zakonik o krivičnom postupku) (the "CPC")
The CPC provides that interception and surveillance of

electronic communications may be employed, as special investigation measures, in pre-formal and formal investigation stages of criminal proceedings, and ordered against a person suspected of committing or preparing a war crime, organized crime, cyber-crime or one of various listed serious crimes (stated in Article 161, paragraphs 2, 3 and 5), if evidence of that crime cannot be collected in any other way, or if gathering evidence by regular investigation measures would cause significant difficulties (Article 161).

The order for interception is issued by the competent criminal court, upon the request of the State Prosecutor for a period of three months with the possibility of an extension of three more months. In cases of war crimes, organized crime and cyber-crime, this maximum six months period may be extended twice, each time for an additional three months (Article 167).

The interception may be performed by the police, the Security-Information Agency or the Military Security Agency (Article 168). If, during the interception, the relevant government agency obtains information indicating that a person uses another phone number or address, the interception may be extended to include the phone number or address by a decision of the director of that government agency, who will also notify the State Prosecutor. The State Prosecutor subsequently files the request for extension with the competent criminal court which will either render a new decision approving the extension or order the destruction of the materials collected (Article 169).

Police Act (Official Gazette of the Republic of Serbia nos. 101/2005, 63/2009 and 92/2011, Zakon o policiji) (the "PA")

The PA authorises the police to intercept electronic communications if such interception is necessary to arrest or apprehend a person under reasonable suspicion of having committed an offence punishable with imprisonment of four or more years and for whom an international arrest warrant is issued, if the police cannot apprehend such a person by other means or when other means would involve disproportionate difficulties.

The request for interception is submitted by the director of the police and approved by the president of the Cassation Court or, in the absence of the president of the Cassation Court, by a judge of the Cassation Court authorised to rule on such a request. Each interception may last up to six months, and may be extended by an additional six months.

Materials collected by an interception may not be used as evidence in criminal proceedings and must be submitted for destruction to the president of the Cassation Court, or the authorised judge of that court, immediately upon completion of the interception. In circumstances in which waiting for the court's approval might jeopardise a police investigation, the interception may be ordered by a decision of the director of the police, with prior written approval of the president of the Cassation Court or the authorised judge of that court. In such cases, the director of the police is obliged to submit to the court a written request for continued interception within 24 hours from obtaining prior approval. The court will decide on the continuation or suspension of the interception within 72 hours of receipt or the request (Article 83).

Security-Information Agency Act (Official Gazette of the Republic of Serbia nos. 42/2002, 111/2009, 65/2014 and 66/2014, Zakon o bezbednosno-informativnoj agenciji) (the "SIAA")

The SIAA provides for secret surveillance and recording of communications or surveillance of an electronic or any other address as special measures which may be employed against a person, group or organization under reasonable suspicion of undertaking or preparing activities which threaten the security of the Republic of Serbia. Such special measures may only be used when the circumstances of the case indicate that the suspected activities could not be discovered, prevented or proved by other means, or that other means would involve disproportionate difficulties or serious danger (Articles 13 and 14). The SIAA does not define serious danger nor specify who should be in serious danger for these provisions to take effect.

Secret surveillance must be requested by the director of the Security-Information Agency and ordered by the president of the Higher Court in Belgrade (the "President"), or a judge of the special department of the Higher Court in Belgrade who handles cases of organized crime, corruption and other serious offences (the "Judge") (Article 15). The interception may be ordered for a period of three months and, if necessary, may be extended up to three times, each time for a period of three months (Article 15a).

If, during the interception, the Security-Information Agency obtains information indicating that the subject of the interception is using other means of communication, the director of the Agency may file a request for extension of the interception to include the discovered means of communications. If the President or Judge adopts this request, a new decision will be rendered approving the extension. If the request is rejected the collected materials must be destroyed (Article 15b).

Military Security Agency and Military Intelligence Agency Act (Official Gazette of the Republic of Serbia nos. 88/2009, 55/2012 and 17/2013, Zakon o vojnobezbednosnoj agenciji i vojnoobaveštajnoj agenciji) (the "MSA")

Under the MSA, the Military Security Agency, which is in charge of security and counter intelligence protection of the Ministry of Defence and Military of the Republic of Serbia (Article 5), is authorised to secretly collect data as a special measure (including interception under the ECA), if data cannot be collected by other means or if collection by other means would cause disproportionate risk to the lives and health of people and property, or disproportionate expense (Articles 11 and 12). Information may be collected for the purpose of preventing threats directed at the Ministry of Defence and the Military of the Republic of Serbia (Article 11, paragraph 2).

This measure can be applied on the basis of a written and reasoned decision of the Cassation Court in response to a request of the Director of the Military Security Agency and may

be ordered for a period of six months, with the possibility of extension by an additional six months. (Articles 14 and 17).

DISCLOSURE OF COMMUNICATIONS DATA

Constitution of the Republic of Serbia (Official Gazette of the Republic of Serbia no. 98/2006, Ustav Republike Srbije) (the "Constitution")
With reference to Article 41 of the Constitution (described above), the Constitutional Court of Serbia issued a decision finding that derogation from the confidentiality of "other means of communications" includes not only interception of communications which would reveal the content of communications, but also the collection of metadata. Consequently, network operators and service providers must only disclose retained metadata on the basis of a court decision in accordance with Article 41 of the Constitution (Decision IUz-1218/2010 of the Constitutional Court of Serbia).

Electronic Communications Act (Official Gazette of the Republic of Serbia nos. 44/2010, 60/2013 and 62/2014, Zakon o elektronskim komunikacijama) (the "ECA")
According to Article 128, paragraph 2, network operators and service providers are obliged to disclose retained metadata to government agencies (the police, the State Prosecutor, the Security-Information Agency and the Military Security Agency) that obtain a court decision allowing them such access for a limited period of time and for the purpose of conducting criminal proceedings or national security.

According to Article 128, paragraph 6 and Article 129, network operators and service providers are obliged to retain for a period of 12 months data:

(a) tracing and identifying the source of a communication;

(b) identifying the destination of a communication;

(c) determining the beginning, duration and end of a communication;

(d) identifying the type of communication;

(e) identifying users' terminal equipment; and

(f) identifying the location of the users' mobile terminal equipment.

Network operators and service providers must retain customers' metadata for a period of 12 months and government agencies are only allowed to request access to such metadata.

Under Article 129, network operators and service providers must not retain the content of customer communications. Since, however, Article 128, paragraph 2, allows interception of electronic communications on the basis of a court decision, if such court decision contains an order for the retention of the content of electronic communications, then network operators and service providers would be obliged to act upon it.

Criminal Procedure Code (Official Gazette of the Republic of Serbia nos. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 and 55/2014, Zakonik o krivičnom postupku) (the "CPC")
Under the CPC, computer data searches of processed personal and other data may be employed as a special investigation measure covering the collection of metadata retained by a network operator or service provider, for the pre-trial and investigation phase of criminal proceedings. These measures may be ordered in relation to a person suspected of committing or preparing a war crime, organized crime, cyber-crime or one of the listed serious crimes, if evidence of that crime cannot be collected in any other way or if gathering evidence by regular investigation measures would cause significant difficulties (Article 178).

The order for a computer data search is rendered by the competent court, upon the request of the State Prosecutor, for a period of three months with the possibility of up to two extensions, each time for an additional three months.

This measure is implemented by the police, the Security-Information Agency, the Military Security Agency, the customs, tax and other state authorities, or legal entities vested with official authority (Article 180).

Police Act (Official Gazette of the Republic of Serbia nos. 101/2005, 63/2009 and 92/2011, Zakon o policiji) (the "PA")
Under the PA, the police are authorised to obtain metadata relating to electronic communications if it is necessary for arresting or apprehending a person who is under reasonable suspicion of having committed an offence punishable with imprisonment of four or more years, and for whom an international arrest warrant is issued, if the police cannot apprehend such a person by other means or when other means would involve disproportionate difficulties.

The request for obtaining metadata relating to electronic communications is submitted by the director of the police and approved by the president of the Cassation Court or, in the absence of the president of the Cassation Court, by an authorised judge of the Cassation Court, within 72 hours of the receipt of the request. This measure may last up to six months, and may be extended by an additional six months.

Security-Information Agency Act (Official Gazette of the Republic of Serbia nos. 42/2002, 111/2009, 65/2014 and 66/2014, Zakon o bezbednosno-informativnoj agenciji) (the "SIAA")
Under the SIAA, obtaining metadata may be ordered as a special measure when the metadata relates to the communications of a person, group or organization under reasonable suspicion of undertaking or preparing activities which threaten the security of the Republic of Serbia, and the circumstances of the case indicate that their activities may not be discovered, prevented or proved by other means or that other means would involve disproportionate difficulties or serious danger (Article 13).

This measure must be ordered by the president of the Higher

Court in Belgrade (the "President"), or a judge of the special department of the Higher Court in Belgrade who handles cases of organized crime, corruption and other serious offences (the "Judge"), upon the request of the Director of the Security-Information Agency (Article 15). The measure may be ordered for a period of three months and if necessary may be extended up to three times, each time for a period of three months (Article 15a).

If disclosed metadata indicates that an individual, group or organization is using other means of communication, the director of the Security-Information Agency may order extension of the special measure and subsequently file a request for extension of a measure in relation to the discovered means of communications. If the President or Judge adopts this request, he/she will render a new decision approving the extension. Where such a request is not adopted, the collected materials must be destroyed (Article 15b).

Military Security Agency and Military Intelligence Agency Act (Official Gazette of the Republic of Serbia nos. 88/2009, 55/2012 and 17/2013, Zakon o vojnobezbednosnoj agenciji i vojnoobaveštajnoj agenciji) (the "MSA")

As mentioned above, under the MSA, the Military Security Agency is authorised to undertake the secret collection of data as a special measure in certain circumstances (Article 11). Secret electronic surveillance of electronic communications with the purpose of obtaining retained traffic data is a special measure requiring a written decision of the Cassation Court, rendered upon the request of the Director of the Military Security Agency and may be ordered for a period of six months, with the possibility of extension for an additional six months (Articles 14 and 17).

Technical Conditions

According to the Technical conditions for subsystems, devices, equipment and installations for mobile telecommunication networks no. 1-01-110-7/08 ("Mobile Technical Conditions"), the Technical conditions for subsystems, devices, equipment and installations for landline telecommunication networks no. 1-01-110-8/08 ("Landline Technical Conditions") and the Technical conditions for subsystems, devices, equipment and installations for internet network no. 1-01-110-19/08 ("Internet Technical Conditions") issued by the Electronic Communications Agency, network operators and service providers are obliged to remove their encryptions prior to delivery of the content of communications or metadata relating to communications to the competent government agencies (section 2 , Mobile and Landline Technical Conditions and Section 6, Internet Technical Conditions).

NATIONAL SECURITY AND EMERGENCY POWERS

Defence Act (Official Gazette of the Republic of Serbia, nos. 116/2007, 88/2009, 88/2009 and 104/2009, Zakon o odbrani) ("DA")

According to the DA, in a state of emergency or a state of war, legal entities in the postal-telegraph-telephone sector and other carriers of telecommunications systems must prioritise the delivery of their services as specified by the Ministry of Defence (Article 73, paragraph 1). The Decision on establishing large technical systems significant for defence (Official Gazette of the Republic of Serbia, no. 41/2014) stipulates that Telenor d.o.o., as well as Telekom Srbija a.d, and VIP mobile d.o.o. are significant technical systems in the field of telecommunications which are required to adjust their systems to the needs of the defence system in Serbia.

Article 202 of the Constitution allows for the introduction of measures which would provide derogation from the general protection given to confidentiality of letters and other means of communication and protection of personal data (under Article 41 of the Constitution) in a state of emergency or war. Government agencies may, on the basis of such measures, require access to a network operator's or service provider's customer communications data and/or network, without adhering to the procedure prescribed for obtaining these data in regular circumstances, that is, without presenting a court decision authorizing interception of electronic communications or access to the retained data.

Measures providing for derogation from Article 41 of the Constitution are adopted by the National Assembly or, if the National Assembly is not in a position to convene, by government decree with the President of the Republic as a co-signatory in the case of a national emergency (Article 200, paragraph 6 of the Constitution) or by the President of the Republic together with the President of the National Assembly and the Prime Minister in the case of a state of war (Article 201, paragraph 4 of the Constitution).

Measures providing for derogation from Article 41 of the Constitution in a state of emergency are effective for a maximum of 90 days, with the possibility of extension under the same terms. Measures providing for derogation from Article 41 of the Constitution in a state of war may continue as long as necessary, as decided by the National Assembly, or the government, if the National Assembly is not in a position to convene.

Police Act (Official Gazette of the Republic of Serbia nos. 101/2005, 63/2009 and 92/2011, Zakon o policiji) (the "PA")

In emergencies, the disclosure of metadata relating to electronic communications may be ordered by a decision of the director of the police, with prior written approval of the president of the Cassation Court or, in the absence of the president of the Cassation Court, by an authorised judge of the Cassation Court, in which case the director of the police is obliged to submit a written request to the Court allowing continued collection of metadata within 24 hours of obtaining prior approval (Article 83).

Military Security Agency and Military Intelligence Agency Act (Official Gazette of the Republic of Serbia nos. 88/2009, 55/2012 and 17/2013, Zakon o vojnobezbednosnoj agenciji i vojnoobaveštajnoj agenciji) (the "MSA")

In emergencies, and particularly in cases of domestic and international terrorism, secret collection of data may be ordered by a decision of the Director of the Military Security Agency, with the interim prior approval of a judge of the Court of Cassation. The decision will subsequently be assessed in more detail and the judge will either grant a continuation of the measure or terminate the measure within 24 hours of its commencement (Article 15).

CENSORSHIP

Enforcement and Security Act (Official Gazette of the Republic of Serbia, nos. 31/2011, 99/2011, 109/2013, 55/2014 and 139/2014, Zakon o izvršenju i obezbeđenju) ("ESA")
There is no provision which explicitly regulates censorship and authorises government agencies to request censorship of customer communications. However, network operators and service providers would be obliged to censor customers' communication pursuant to the ESA, if such order were given by a competent court in the form of an interim measure or in the form of a final court decision.

Electronic Commerce Act
(Official Gazette of the Republic of Serbia, nos. 41/2009 and 95/2013, Zakon o elektronskoj trgovini)

According to the Electronic Commerce Act, internet service providers are obliged to implement court decisions on blocking IP addresses or restricting access to certain information society services provided by them (Article 21a). In addition, network operators that provide internet services to their customers are obliged to block IP addresses if an order is issued by a competent court in accordance with the ESA or in a final court decision rendered in both criminal and civil proceedings.

Electronic Communications Act (Official Gazette of the Republic of Serbia nos. 44/2010, 60/2013 and 62/2014, Zakon o elektronskim komunikacijama) (the "ECA")
Article 127, paragraph 3, prohibits network operators and service providers from publishing records on requests received for interception which contain data identifying an authorised person who conducted the interception, the decision which provided the legal basis for interception and the date and time of the interception.

OVERSIGHT OF THE USE OF POWERS

Judicial Oversight
Interception of electronic communications conducted by all government agencies authorised to undertake such interception and retention of the content of electronic communications are overseen by the competent court which ordered the measure and monitors its enforcement (Article 126, paragraph 1 and Article 128, paragraph 2 ECA; Articles 166 and 286 CPC; Article 83, paragraph 2 PA; Articles 15 and 16 SIAA; Articles 14 and 15 MSA). If materials obtained by interception were not collected in accordance with the prescribed procedure, the competent court will order their destruction (Article 163 CPC; Article 15b SIAA; Article 15 MSA).

Electronic Communications Act (Official Gazette of the Republic of Serbia nos. 44/2010, 60/2013 and 62/2014, Zakon o elektronskim komunikacijama) (the "ECA")
The ECA contains provisions concerning the general oversight of network operators' and service providers' operations by the Agency for Electronic Communications (the "Agency") and the Inspectorate of the Ministry of Trade, Tourism and Telecommunications (the "Inspectorate").

At the request of the Agency, network operators and service providers are obliged to submit information on the protection of customers' personal data and privacy (Article 41) and to correct irregularities in its technical and organizational settings (enabling interception) identified by the Agency and to inform the Inspectorate if a network operator or service provider does not comply with its request (Article 131).

The supervision of network operators and service providers is also conducted by the Inspectorate (Article 132 and Article 134, paragraph 1, subparagraph 6), which is authorised to order a network operator or service provider to remedy irregularities, oversights or omissions in its work within a given period of time (Article 135, paragraph 1, subparagraph 1).

The Ministry of Trade, Tourism and Telecommunications also monitors network operators' and service providers' assistance in implementing interception capabilities (Article 132 and Article 134, paragraph 1, subparagraph 6) and is authorised to order network operators and service providers to implement such capabilities within a given period of time and to temporarily suspend their activities if they do not comply (Article 135, paragraph 1, subparagraphs 1 and 3).

Network operators, service providers and government agencies are obliged to submit records in relation to requests received to access retained data in the preceding year on 31 January of each year to the Commissioner for Personal Data Protection. The Commissioner is authorised to order certain measures if data processing was not in accordance with the law (Articles 44, 45 and 56 of PDPA).

Police Act (Official Gazette of the Republic of Serbia nos. 101/2005, 63/2009 and 92/2011, Zakon o policiji) (the "PA")
According to Article 171, police activities are generally supervised by a special department of the Ministry of Police – the Division of Internal Control, which monitors the legality of police work, especially with regards to respect and protection of human rights in the performance of police tasks and applying police powers.

Military Security Agency and Military Intelligence Agency Act (Official Gazette of the Republic of Serbia nos. 88/2009, 55/2012 and 17/2013, Zakon o vojnobezbednosnoj agenciji i vojnoobaveštajnoj agenciji) (the "MSA")
Article 57 provides for internal control of the Military Security Agency, conducted by the Division of Internal Control of the Military Security Agency. There is also political supervision over the work of the police, the Security–Information Agency and

the Military Security Agency by the National Assembly and the government (Article 17 SIAA and Article 57 MSA).

Constitution of the Republic of Serbia (Official Gazette of the Republic of Serbia no. 98/2006, Ustav Republike Srbije) (the "Constitution")
The Constitutional Court of Serbia, which is authorised to assess constitutionality and legality of laws and other general acts, may find that a measure of derogation from confidentiality of letters and other means of communication and protection of personal data introduced during a state of war or emergency is unconstitutional (Article 168).

Law on Constitutional Court of Serbia ("Official Gazette of the Republic of Serbia, nos. 09/2007, 99/2011 and 18/2013, Zakon o ustavnom sudu)
Network operators and service providers may file a constitutional appeal against a decision of a government agency as an individual act which violates Constitutional guarantees, when other legal remedies have been exhausted or are not prescribed or where the right to their judicial protection has been excluded by law (Articles 82 and 83).

PUBLICATION OF AGGREGATE DATA RELATING TO THE USE OF GOVERNMENT POWERS

There is no law prohibiting the publication of any of the laws mentioned in this report or any description of the powers set out in any of those laws.

Electronic Communications Act (Official Gazette of the Republic of Serbia nos. 44/2010, 60/2013 and 62/2014, Zakon o elektronskim komunikacijama) (the "ECA")
Article 27, paragraph 3 of the ECA prevents network operators and service providers from publishing records of requests for interception or access to metadata that provide information on: the identity of the persons conducting the interception or who gained access to the metadata, the identity of the people whose communications were intercepted or whose metadata was accessed, the purpose of the interception or access, or the time and place of the interception or access.

This would not, however, prevent network operators or service providers publishing aggregate data on the number of requests to intercept communications for example, provided that none of the above information is included in this publication.

Law stated as at 20 January 2015.

SWEDEN – 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 Swedish law.

PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

Electronic Communications Act 2003 (2003:389) (lag (2003:389) om elektronisk kommunikation) (the "ECA")

According to chapter 6, section 17, it is prohibited to intercept content data or monitor metadata associated with an electronic message.

However, under chapter 6, sections 19 and 21, network operators and service providers are subject to obligations to:

(a) conduct their business, and adapt and construct their network, in a manner that enables the execution of court orders for secret interception of electronic communications messages; and

(b) conduct their business in a manner that enables the execution of such court orders for secret interception without disclosure of such interceptions.

The content of an intercepted message must be made available in a form that can be easily processed by the government agency requesting the interception.

Chapter 6, section 19(a), requires network operators and service providers that own cables through which electronic signals are transmitted over the Swedish border, to transmit such signals to certain interaction points chosen by the network operator or service provider. The network operator or service provider must notify the National Defence Radio Establishment (Försvarets radioanstalt) (the "NDRE") of the location of the interaction points. This serves the purpose of allowing the Inspection of Defence Intelligence (the "IDI") to gain technical access to the electronic signals at the interaction points, in accordance with the Defence Signals Intelligence Act (2008:717) (lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet) (the "DSIA").The IDI then transmits some of the signals on to the NDRE, in accordance with the DSIA.

In accordance with sections 5, 5(a) and 12 DSIA, the NDRE must present a court order from the Defence Intelligence Court mandating the monitoring of the electronic signals in question. The IDI does not, however, need to present a court order to require access to all the electronic signals passing through the interaction points. Consequently, the relevant network operator or service provider is obliged to give the IDI access to the cable based electronic signals that pass through an interaction point, without court orders or warrants.

The NDRE is responsible for the actual construction of the interaction point, as well as for securing technical access to the signals at the interaction point and further transmitting them to its own systems. While the network operator or service provider is obliged to bear the costs associated with the transmission of the signals to the interaction point, the NDRE bears the costs associated with the operation of the interaction point.

These requirements fall under the remit of defence intelligence conducted to support the Swedish foreign, security and defence policies and for mapping external threats to the country.

Chapter 6, section 19(a) also obliges any network operator or service provider that carries signals over the Swedish borders through cables to disclose to the NDRE any information in its possession that makes it easier for the NDRE to manage and intercept the signals accessed at an interaction point, for example, the title, architecture, bandwidth, or direction of the connections and the type of signalling. The obligation applies to all network operators or service providers that carry cross-border signals, and not only to the network operators and service providers that own the cables.

Code (1942:740) of Judicial Procedure (Rättegångsbalk (1942:740) (the "CJP")
Pursuant to chapter 27, section 21, the general obligation for network operators and service providers to provide interception assistance is qualified by the requirement that the requesting government agency obtains and presents a court order authorising interception. The request must be submitted to the competent court by a public prosecutor. According to chapter 27, section 18, a request for interception may only be granted in investigations relating to certain serious crimes. In this context, "serious crimes" include crimes for which the prescribed minimum penalty is imprisonment for two years or more, and offences such as sabotage, arson, espionage, and terrorism.

In addition, a court order will only be granted if the conditions set out in chapter 27, section 20 are fulfilled. Section 20 states that the use of interception must be of exceptional importance for the purpose of facilitating the criminal investigation in question. The court order may only concern a particular number, address or the electronic communications equipment possessed by an individual who can reasonably be suspected of committing the crime under investigation. It may concern another individual, if there are particular reasons to believe that they will be contacted by the suspect.

According to chapter 27, section 21(a), if the public prosecutor responsible for the investigation deems that awaiting the court order would result in a delay of material importance to the investigation, the public prosecutor may himself, without first obtaining a court order, render an interim order regarding secret interception. In such cases, the public prosecutor should inform the court of its decision following which the court must promptly evaluate the interim order. If the court does not find reasons to support the decision, it must revoke the earlier decision, in which case no information collected under the interim order may be used in the investigation, if such information is detrimental to the person concerned.

Under chapter 27, section 22, it is prohibited to intercept communications involving information entrusted to certain individuals in their professional capacity. Such individuals are those who, according to chapter 36, section 5, are prohibited from disclosing information mentioned in the conversation. Examples of such individuals include advocates, physicians and freelance journalists, in relation to their sources.

DISCLOSURE OF COMMUNICATIONS DATA

Electronic Communications Act 2003 (2003:389) (lag (2003:389) om elektronisk kommunikation) (the "ECA")
According to chapter 6, section 20, all data relating to customer communications, including metadata and content data, are confidential and may not be disclosed to anyone other than the participants of the relevant communication.

However, according to chapter 6, section 22, confidentiality does not apply in the following situations, where the network operator or service provider must disclose:

- customer subscription details, upon request from any government agency, where they are needed for serving a person in accordance with the Service of Process Act (2010:1932) (delgivningslag (2010:1932)), if it could be expected that the person sought to be served is hiding or if there otherwise are exceptional reasons for such disclosure;
- customer subscription details, which relate to a suspected crime, upon request from the Public Prosecution Authority (Åklagarmyndigheten), the Police Authority (Polismyndigheten), the Swedish Security Service (Säkerhetspolisen) or any other government agency investigating a suspected crime;
- customer subscription details relating to a customer and other information relating to a specific electronic message, including information about the geographic area in which the relevant communication equipment is or has been situated, upon request from the Police Authority. The Police Authority can only make such a request to assist in the search for a person who has gone missing in circumstances which suggest their life is in danger or that they are at serious risk of harm;
- customer subscription details, upon request by the Enforcement Authority (Kronofogdemyndigheten), if needed in an enforcement process (meaning collection of debts or actions related to such enforcement) and the Enforcement Authority deems such information to be of material importance to the processing of a certain matter;
- customer subscription details, upon request by the Tax Agency (Skatteverket), in the event such information is of material importance to the processing of any matter relating to the calculation of tax owed, payment of tax-related charges or any matter relating to correct registration of address or domicile in accordance with the National Registration Act (1991:481) (folkbokföringslag (1991:481));
- customer subscription details, upon request from the Police Authority, if such information is needed for providing notification, obtaining information or identifying persons in relation to accidents or casualties, or when investigating such accidents or casualties, or when the Police Authority leave a person aged under 18 to the social services in accordance with section 12 of the Police Act (1984:387) (polislag (1984:387));
- customer subscription details, upon request by the Police Authority or the Public Prosecution Authority, if such authority determines such information is necessary in order for the authority to be able to inform a guardian in accordance with Section 33, of the Act (1964:167) on Juvenile Criminals (lagen (1964:167) om särskilda bestämmelser om unga lagöverträdare); and
- customer subscription details and other information relating to a specific electronic message, upon request by a regional emergency service centre (regional alarmeringscentral) in accordance with the Act

(1981:1104) on Regional Emergency Service Centres (lagen (1981:1104) om verksamheten hos vissa regionala alarmeringscentraler).

A request under section 22 of the ECA does not require a court order or any particular decision by the relevant government agency. This is in contrast to when requests are made pursuant to the Act on Collection of Data in Electronic Communication in the Crime Combatting Authorities' Intelligence Services (as described below).

Under chapter 6, section 16(c) ECA, a government agency may only request metadata retained by a network operator or service provider under chapter 6, section 16(a), in the following situations:

(a) a network operator or service provider must, upon request from the Public Prosecution Authority, the Police Authority, the Swedish Security Service or any other government agency, in connection with an investigation of a crime, disclose customer subscription details pursuant to chapter 6, section 22;

(b) pursuant to a court order sought by a public prosecutor under chapter 27, section 21 CJP, network operators and service providers are, pursuant to Chapter 27, Section 19 CJP, required to disclose to the Police Authority, the Swedish Security Service or the Customs Agency (Tullverket) the following metadata (as detailed in the court order):

(i) information on messages which have been transmitted across an electronic telecommunications network or which have been transmitted to or from a telephone number or other address;

(ii) what electronic communication devices that have been present within a certain geographic area; and

(iii) in what geographic area a certain electronic communication device is or has been present.

According to chapter 6, sections 16(a) to 16(f), a network operator or service provider must retain customer subscription details and other information relating to a certain electronic message, which are necessary to track and identify: the source of the communication; the ultimate destination of the communication; date, time and duration of the communication; type of communication; communication equipment; and localisation of mobile communication equipment at the commencement and end of the communication. Network operators and service providers are also obliged to retain data relating to failed calls or connections, in relation to which the network operator or service provider shall retain the data generated or processed.

The specific information which should be retained by the network operator or service provider is clarified further in sections 38 to 43, of the Ordinance (2003:396) on Electronic Communication (förordning (2003:396) om elektronisk kommunikation) (the "OEC"). In addition, under section 44 OEC, the Swedish Post and Telecommunication Authority (Sw. Post- och telestyrelsen) (the "PTA") may stipulate more detailed requirements relating to stored data.

The PTA, under exceptional circumstances, may also create exemptions from the obligation to retain data (chapter 6, section 16(b) ECA). In such event, the PTA will consult with the Public Prosecution Authority, the Police Authority and the Swedish Security Service (section 45 OEC).

According to chapter 6, section 16(d) ECA, data retained in accordance with chapter 6, section 16(a) ECA, must be retained for six months from the date the communication ended. After this period the network operator or service provider must permanently delete the retained data.

It should be noted that chapter 6, sections 16(a) to 16(f), implement Directive 2006/24/EC of the European Parliament and of the Council (the "Data Retention Directive"), which on 8 April 2014 was declared invalid by the Court of Justice of the European Union. The validity of the data retention obligations of network operators and service providers described above has, as a consequence, been contested by certain network operators and service providers operating in Sweden. The validity of the Swedish implementation of the Data Retention Directive is currently being tried in Swedish courts.

On 13 October 2014, the Administrative Court of Stockholm held that the Swedish implementation of the Data Retention Directive is lawful and does not contravene any of the principles outlined by the European Court of Justice in its judgment. This judgment has been appealed and is being examined by the Administrative Court of Appeals in Stockholm. Hence, currently, the Swedish data retention obligations remain valid, but there is an uncertainty as to whether the obligations will remain in their present form.

According to page 27 of the legislative preparatory works to the Telecommunications Act ((telelag) (1993:597) (replaced by the ECA) and (prop. 1995/96:180 – teleoperatörernas skyldigheter vid hemlig teleavlyssning och hemlig teleövervakning)), the network operator or service provider's obligations in relation to secret telecommunication interception and secret telecommunication supervision include a responsibility to decrypt data that has been encrypted by the network operator or service provider. According to the subsequent legislative preparatory works (drafted in relation to the ECA), the legislator did not intend for a factual change in relation to these provisions, and therefore, the specific obligation to decrypt data is most likely still in force.

Moreover, although not a formal requirement, the opinion of the Swedish Security Service is that the information must be processed automatically and made available in a standardised form, namely ITS27, in order for the network operator or service provider to conform to the requirements in ECA.

Code (1942:740) of Judicial Procedure (Rättegångsbalk (1942:740) (the "CJP")

According to chapter 27, section 21(a), if the public prosecutor

deems that awaiting the court order would result in a delay of material importance for the investigation, the public prosecutor may permit the disclosure of information. In such a scenario, the public prosecutor must inform the court of its decision, following which the court must promptly evaluate the interim order permitting the disclosure. If that the court does not find reasons to uphold the decision, it must revoke the decision, and no information collected under the initial interim order may be used in the investigation, if such information is detrimental to the person concerned.

Act (2012:278) on Collection of Data in Electronic Communication in the Crime Combatting Authorities' Intelligence Services
(lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet) (the "IEUK")

Following a decision from the Police Authority, the Swedish Security Service or the Customs Agency, made by a duly authorized representative (meaning the head of the agency or a person to which the head of the agency has delegated the right), a network operator or service provider must, in accordance with section 1, disclose the metadata outlined under chapter 27 of the CJP summarised in paragraph 2.1 (b) above.

According to section 2, information may only be collected if:

(a) the collection is of particular importance in order to prevent or discover criminal activities which involve any crime which is sanctioned with no less than two years imprisonment; and

(b) the reasons for the collection outweigh the interests of the person in relation to which the measure is targeted. A court order will be required in accordance with chapter 27, section 21 CJP (as described above).

NATIONAL SECURITY AND EMERGENCY POWERS

Electronic Communications Act 2003 (2003:389) (lag (2003:389) om elektronisk kommunikation) (the "ECA")
Under chapter 7, section 8 if a network operator or service provider does not fulfil its obligations under the ECA, and such breach severely threatens public order, national security or public health or could otherwise be deemed to cause severe economic or operational problems for the supplier or a user of electronic communication networks or services, then the Swedish Post and Telecommunication Authority (the "PTA") may, with immediate effect, order an injunction against the relevant network operator or service provider.

Such decision may be valid for a maximum of three months. If any correction measures are not taken by the network operator or service provider, the period may be extended by a further three months.

The PTA may also revoke a network operator or service provider's authorisation to use a certain radio transmitter or to use radio transmitters within certain radio frequencies in its business. It may change the terms and conditions of such authorisations.

In accordance with chapter 1, section 8, if Sweden is (or has recently been) at war or under the threat of war, or if there are extraordinary conditions that are caused by a war outside of Sweden, the government may issue regulations governing electronic communications networks and associated facilities and services, and other radio usage as necessary with regard to national defence or security in general. This may result in additional emergency powers for the relevant authorities.

Proposed Swedish Government Official Report (SOU 2013:33 – en myndighet för alarmering) (the "Report")
The Report provides that certain government agencies will be able to send text messages alerting citizens in emergency situations. The Report defines which government agencies are to have the right and who is responsible for the costs they entail.

Further legislative discussion
There are theoretical discussions indicating that the government, under exceptional circumstances (for instance severe threats against national security), would have the right to invoke a constitutional privilege of self-defence (konstitutionell nödrätt) that may entail a wider scope of governmental power than otherwise described in this report. In accordance with page 95 of the preparatory works (SOU 2003:32 – Vår beredskap efter den 11 september: betänkande), the right to act in emergency situations is covered by Chapter 1-12 of the Swedish Form of Government (Regeringsformen (1974:152)), where the parliament's functions are delegated to the government. In situations where delegation powers under the aforementioned chapters do not exist, one option to act is through the constitutional privilege of self-defence.

The constitutional privilege of self-defence has never been exercised, thus making it difficult to properly assess its scope in this context. It is, however, not unlikely that the government may take control of a network operator or service provider's network if necessary to uphold national security.

CENSORSHIP

Freedom of Press Regulation (tryckfrihetsförordning (1949:105)) and the Freedom of Speech Constitution (yttrandefrihetsgrundlag (1991:1469))
Under the Freedom of Press Regulation and the Freedom of Speech Constitution, there is a prohibition against censorship. The right to express an opinion, without it being censored, is thus a constitutional right in Sweden.

Code (1942:740) of Judicial Procedure (Rättegångsbalk (1942:740) (the "CJP")
As described above, under chapter 27, section 19, data may be secretly intercepted via real-time interception of electronic communications.

Government agencies have the right to prevent the customer communications detailed in this section (described above) from reaching its recipient in an investigation for offences such as hacking, child pornography and drug offences.

Government agencies also have the right to switch off a phone number in critical situations to prevent a suspect from connecting his or her accomplices or receiving warning calls.

Electronic Communications Act 2003 (2003:389) (lag (2003:389) om elektronisk kommunikation) (the "ECA")
Under chapter 7, section 9, the Consumer Ombudsman (Konsumentombudsmannen) may order a network operator or service provider to prevent user access to a number whose digit structure lacks a geographical sense, if the marketing of the number or the service related to it is improper or if material information is omitted in the marketing material. This means that it may become impossible for users to reach the number or service.

Certain Internet Service Providers have entered into voluntary cooperation agreements with the Police Authority to block IP addresses that contain child pornography material. The content and scope of such agreements are confidential.

Moreover, an internet service provider has recently been sued for assisting an IP-infringement when refusing to block illegal streaming sites' IP addresses. The outcome of this case should make it clearer whether or not a government agency may require a network operator or service provider to block IP addresses in certain circumstances.

OVERSIGHT OF THE USE OF POWERS

Judicial Oversight
Where a court order is required for interception or the collection of information pursuant to a court under chapter 27, section 21 CJP, the competent court and the relevant public prosecutor have a supervisory role in the use of these measures.

The Swedish Post and Telecommunication Authority (Post- och telestyrelsen) (the "PTA")
The PTA generally supervises network operators' and service providers' compliance with their respective obligations. According to chapter 7 of the ECA, the PTA is entitled to order a network operator or service provider to disclose information and documentation needed in order to ensure that the network operator or service provider complies with its obligations. Such order may be combined with a conditional fine. The PTA is also entitled to gain access to any facilities (excluding residences) where a network operator or service provider's business is conducted in order to perform an audit.

If the PTA deems that a network operator or service provider has breached its obligations, then the PTA may order the network operator or service provider to rectify its breach. Such order may be combined with a conditional fine.

Inspection of Defence Intelligence (the "IDI")
The IDI supervises the secret defence intelligence activities performed by the (National Defence Radio Establishment) (the "NDRE"), for instance by only permitting the NDRE to intercept signals which are covered by a court order from the Defence Intelligence Court (Försvarsunderrättelsedomstolen).

Commission on Security and Integrity Protection (Säkerhets- och integritetsskyddsnämnden) (the "SIN")
All decisions on the collection of data under the Act on Collection of Data in Electronic Communication in the crime combatting Authorities Intelligence Services ("IEUK") shall be communicated to SIN, which supervises the relevant government agencies' compliance with the IEUK.

PUBLICATION OF AGGREGATE DATA RELATING TO USE OF GOVERNMENT POWERS

Restrictions on network operators and service providers Publicity and Secrecy Act (offentlighets- och sekretesslagen (2009:400)) (the "PSA")
Under the PSA, the government has the legal authority to prevent a network operator or service provider from publishing aggregate data relating to intercept requests or acquisitions of metadata when, for example, secrecy under a current investigation applies to the aggregate data and publication of the information may jeopardise or impair an investigation. Confidentiality will apply to activities such as those which aim to prevent, detect, investigate or prosecute crime, conducted by prosecutors, the police and the Swedish Security Service among others.

Neither the public prosecutor nor the Police Authority need obtain any authority or court order for the information to be considered confidential.

Confidentiality may also apply to data relating to preliminary investigations in criminal cases or a matter relating to the use of coercive measures, if the purpose of the measures is undermined by disclosure, or if future operations may be damaged by disclosure.

The government does not have the legal authority to prevent a network operator or service provider from publishing descriptions of, or information relating to, the laws described in this report.

Aggregate data published by government agencies.
The Public Prosecution Authority annually publishes a report of the use of secret surveillance-related laws which is available here: http://www.riksdagen.se/sv/Dokument-Lagar/Forslag/Propositioner-och-skrivelser/Redovisning-av-anvandningen-av_H20336/?text=true

Law stated as at 19 January 2015.

THAILAND – 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 Thailand.

Following a coup d'état on 22 May 2014, Thailand is currently governed by the interim government under the peacekeeping power of the National Council for Peace and Order (a military junta). A state of martial law which had been imposed since the beginning of the coup was lifted on 1 April 2015 and immediately replaced by NCPO Order No. 3/2558 (3/2015) re: Maintaining Public Order and National Security issued under Section 44 of the Interim Constitution for an indefinite period of time.

Section 1 to 3 of this report summarises the laws which apply to surveillance and censorship powers in ordinary times. Section 4 explains how military rule affects the implementation of these laws on a legislative basis.

PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

Constitution of the Kingdom of Thailand (Interim) B.E. 2557 (2014) (the "Interim Constitution")

Following the coup d'état, the National Council for Peace and Order issued the Interim Constitution and repealed the Constitution of the Kingdom of Thailand 2007 (the "2007 Constitution"). The 2007 Constitution protected communications from access, interception and disclosure, but provided certain exceptions for government authorities, for example, in relation to national security or public order. As the 2007 Constitution has now been repealed, these protections are no longer guaranteed.

Section 4 of the Interim Constitution recognises that any human rights and freedoms customarily recognised in Thailand and any rights recognised under international obligations are protected under the Interim Constitution. The Interim Constitution does not explain what those rights "customarily recognised in Thailand" include.

Computer Crimes Act B.E. 2550 (2007) (the "CCA")

The scope of the CCA deals with offences committed against computer systems or computer data, and content offences which are already crimes under the Thailand Penal Code (the "Penal Code") and are committed via a computer. The CCA applies to service providers and is overseen by the Ministry of Information and Communication Technology ("MICT").

The scope of the CCA extends to those committing an offence under the CCA outside of Thailand, both Thai citizens and foreign citizens (Section 17 CCA). Such offenders may be penalised within Thailand.

Under section 18(4)-(8) CCA, a competent official (one appointed by the MICT), is empowered to:

- copy computer data or traffic data from a computer system which is reasonably suspected of being used for an offence,
- inspect or access a computer system, computer data, computer traffic data or computer data storage equipment,
- order the person in possession or control of such data equipment to deliver it to him; and
- to seize or attach any computer system for the purposes of gathering evidence in an investigation.

Section 18(7) CCA also authorises a competent officer to decrypt encrypted computer data, to order concerned persons to decrypt encrypted computer data, and/or to order concerned persons to cooperate with a competent officer in decrypting computer data.

"Computer data" means data, statements, or sets of instructions contained in a computer system, the output of which may be processed by a computer system including electronic data.

"Computer traffic data" means data related to computer system-based communications showing sources of origin, starting points, destinations, routes, time, dates, volumes, time periods, types of services or others related to that computer system's communications.

Although section 18 CCA does not refer expressly to "interception" there is no judicial or statutory guidance on the MICT's powers under this section. It may be interpreted widely to include, for example, the ability to conduct direct interception, to require interception assistance or to gain direct access to a network operator or service provider's system.

Under section 19 CCA, the powers under section 18(4)(8) may only be applied if the competent official first makes an application to the competent court.

The application must identify the grounds on which it is believed that an offender is committing or is going to commit an offence under the CCA, the reason for requesting the authority, the characteristics of the alleged offence, a description of the equipment used to commit the alleged offence and details of the offender, to the extent that this is possible.

If the court approves the application, and before taking any further action, the official must send a memorandum explaining the grounds on which the application has been granted to the owner or person in possession of the computer system. Within 48 hours of starting the operation in question, the official must also submit a copy of the memorandum and an explanation of the rationale of the operation to a court with jurisdiction.

The use of section 18(4) (copying of computer data) must not excessively interfere with or obstruct the business operation of the owner or person in possession of the computer data.

Furthermore, in relation to seizure or attachment under section 18(8), the official must issue a letter of seizure or attachment to the person who owns or possesses that computer system as evidence. The seizure or attachment must not last longer than thirty days. If a longer time period is required, a petition must be filed at a court with jurisdiction for permission to extend the time period. The court may allow several extensions, but together they must not exceed sixty days.

When that seizure or attachment is no longer necessary, or upon its expiry date, the competent official must immediately return the computer system that was seized or withdraw the attachment.

Although intercept powers may be inferred from other pieces of legislation (outlined below), the relatively simple process provided for under the CCA means that it is likely to be the legislation under which an interception is most often conducted.

Proposed Amendment to the CCA (the "Proposed Amendment")

On 7 January 2015, the Cabinet approved eight digital and computer-related draft laws aimed at creating a conducive environment for building the digital economy, controlling radio spectrum frequency allocation, and conducting surveillance on people.

The draft bills will be lodged with the National Legislative Assembly for further consideration and may be subject to amendment.

Organisation to Assign Radio Frequency and to Regulate the Broadcasting and Telecommunication Services Act, B.E. 2543 (2000) (the "NBTCA")

Under the NBTCA, on the grounds of public order, or public security, the National Broadcasting and Telecommunications Commission is empowered to issue a provisional order to the competent authority to seize, put to use, prohibit the use of, or prohibit the removal of, radio communication equipment, or part thereof, within the period and under the conditions specified in the order.

Special Case Investigation Act B.E. 2547 (2004) (the "SCIA")

Under section 21, powers under the SCIA may be invoked in relation to criminal cases which involve the violation of specified laws and which have particular characteristics, including those which are particularly complex, those with relevance to national interests, those with involvement of influential people, or cases otherwise selected by the Special Case Board (the "SCB"). Such cases are referred to as Special Case Offences. The relevant laws set out in the Annex to the SCIA include violation of the Law on Loans Amounting to Public Cheating and Fraud, the Competition Act, the Public Company Act, and the Copyright Act.

The SCB is constituted under section 5 SCIA and consists of a number of government ministers and Cabinet-appointed experts chaired by the Prime Minister. Its duties are found under section 10 SCIA and include: the duty to advise the Cabinet regarding the determination of special cases, determining the details of a special offence, and the monitoring and assessment of results of compliance with the SCIA.

Under section 25 SCIA, Special Case Inquiry Officials ("SCIO") (officials working directly for the Department of Special Investigation under the Ministry of Justice) may access and acquire any documents or information sent by a means of communication or any IT media which has been or may be used to commit a Special Case Offence.

The SCIA may therefore apply to network operators and service providers if there is cause to believe that an individual being investigated for a crime under the SCIA has used their services to commit a Special Case Offence.

The SCIO must obtain a court order from the Chief Justice of the Criminal Court (the "Chief Justice") prior to the use of the powers under SCIA.

When granting a court order, the Chief Justice will consider the effect on the rights of the different parties involved and the application overall in light of the following conditions:

(c) there are reasonable grounds to believe that a Special Case Offence is or will be committed;

(d) there are reasonable grounds to believe that access to the information will result in gathering relevant information in relation to a Special Case Offence; and

(e) there are no more appropriate or efficient methods.

The Chief Justice may grant permission for use of the powers for a period of up to 90 days. The network operator or service provider can be required to assist with any decryption of acquired encrypted data under the terms of the court order.

Cyber Security Bill (the "Bill")

The Bill is currently pending approval from the National Legislative Assembly. It proposes to establish a National Cyber Security Committee charged with detecting and countering

online threats to national security, stability, the military and economy.

Under section 35 of the Bill, the Committee would be authorised to access information on personal and other electronic devices without requiring a court order for the purpose of fulfilling its cyber security duties.

DISCLOSURE OF COMMUNICATIONS DATA

Computer Crimes Act B.E. 2550 (2007) (the "CCA")
Under section 18(1)-(3), for the purpose of an investigation and the gathering of evidence in relation to an offence under the CCA, a competent official (one appointed by the Minister of Information and Communication Technology) is given a range of powers including the powers to summon any person related to the offence to give a statement, to procure computer traffic data relating to the relevant communications from a service provider or from other relevant persons, and to request documents and other evidence from the person(s) concerned.

There is no requirement of a court order for use of these powers.

Under section 26 CCA, a service provider must store computer traffic data (described in section 1 above) for at least 90 days from the date on which the data is input into a computer system. However, if necessary, a relevant competent official may, on a case by case basis, instruct a service provider to store data for a period longer than 90 days but not exceeding one year.

Section 17 CCA makes it clear that the provisions of the CCA apply to offences committed outside Thailand.

Proposed amendment to the CCA (the "Proposed Amendment")
The Proposed Amendment, currently sitting with the National Assembly, may see the approval of eight digital and computer-related draft laws.

Section 27(4) of the Proposed Amendment provides that disclosure of personal data without prior consent from the person to which the personal data relates can be made if the public official has a reasonable ground of suspicion that such personal data would concern national security or the security of international affairs.

The Proposed Amendment also seeks to extend the time limit for retention of data provided under section 26 CCA from 90 days (or a maximum of one year) to two years.

Telecommunications Business Act B.E. 2544 (the "Telecommunications Business Act")
The TBA is applicable to telecommunications operators. Under section 50 TBA, telecommunications licensees must keep personal data of their service users for the last three months and, in the event that the service is terminated, to retain this data for three months following the date of termination of the service.

Special Case Investigation Act B.E. 2547 (2004) (the "SCIA")
Disclosure of data, including disclosure of metadata relating to customer communications, may be provided in accordance with section 25 SCIA (as described in section 1.5 above), provided that a court order is obtained first.

CENSORSHIP

The Cyber-Inspector Group (the "CIG")
The Ministry of Information and Communication Technology (the "MICT") was created in Thailand in 2002. One of the MICT's main priorities has been internet regulation, implemented through an MICT unit originally known as CIG. This unit monitors websites for harmful content, facilitates the enactment of legislation governing electronic transactions, and conducts training for personnel to combat cyber terrorism.

Computer Crimes Act B.E. 2550 (2007) (the "CCA")
Under section 20, where information is deemed to negatively affect national security (including lèse majesté, explained below) or may violate public order or good morals (such as pornography), the authorised officials may, with the approval of the Minister of the MICT, petition the relevant court with jurisdiction to halt the dissemination of information directly, or to order a service provider to do so.

Lèse majesté is an offence against the dignity of the reigning sovereign of Thailand. Lèse majesté provisions under Thai law are included in section 2 of the Interim Constitution which stipulates that "the King shall be enthroned in a position of revered worship and shall not be violated. No person shall expose the King to any sort of accusation or action".

Lèse majesté is also classified under section 112 of the Penal Code, (Offences Relating to the Security of the Kingdom).

Section 14 CCA, also provides for a variety of offences which may be relevant to censorship, including:

(i) inputting into a computer system forged or false data in a manner likely to cause injury to another person or to the public;

(ii) inputting false data in a manner likely to damage national security or to cause public panic;

(iii) inputting data constituting an offence against national security under the Penal Code;

(iv) inputting any data of pornographic or obscene nature which is publicly accessible; or

(v) disseminating or forwarding any of the above types of data in the knowledge that the inputting of such data constitutes an offence.

Section 15 CCA, allows the authorities to censure any service provider which intentionally supports or consents to the commission of an offence under section 14 by imposing a jail

term not exceeding five years and/or a fine not exceeding 100,000 Thai baht.

Proposed amendment to the CCA (the "Proposed Amendment")
In the Proposed Amendment, the liability of a service provider under section 15 CCA may be reduced. The Proposed Amendment provides for the Minister of MICT to provide regulations on actions which service providers should take to prevent the dissemination of certain computer data and for the Minister to order the destruction of such computer data. Under the amended section 14 CCA, if the service provider can prove that it acted in accordance with the Minister's instructions, it will not be liable under section 15 CCA.

National security and emergency powers
The legislation provided above describes Thai law in ordinary times. Thailand is currently governed by the interim Government under the peacekeeping power of the NCPO. As a result, NCPO Order No. 3/2558 (3/2015) re: Maintaining Public Order and National Security issued by the Head of the National Council for Peace and Order (the "NCPO") under Section 44 of the Interim Constitution and the Interim Constitution 2014 (both described below) currently supersedes the legislation described above.

Constitution of the Kingdom of Thailand (Interim) B.E. 2557 (2014) (the "Interim Constitution")
Section 44 of the Interim Constitution provides the NCPO with wide powers to take any extrajudicial action it deems necessary against any act which undermines public peace and order or national security. Under section 44, it may suspend or take action, regardless of its effect on the legislative or executive arms of the government or the judiciary, in situations where it is necessary for the benefit or reform in any field and to strengthen public unity and harmony, or for the prevention, disruption or suppression of any act which undermines public peace and order, national security, the monarchy, national economics or the administration of state affairs.

NCPO Order No. 3/2558 Re: Maintaining Public Order and National Security ("Order No. 3/2558")
Following the termination of martial law on 1 April 2015, the NCPO issued NCPO Order No. 3/2558 under Section 44 of the Interim Constitution. It implements measures to deal with actions intended to undermine or destroy peace and national security, violate notifications or orders issued by the NCPO.

NCPO Order No. 3/2558 deals primarily with the maintenance of public order and national security. In particular it gives extensive legal powers to certain categories of military officers that it refers to as "Peacekeeping Officers". The breadth of its provisions and the exact manner in which such provisions may be exercised remains unclear.

NCPO Order No.3/2558 provides Peacekeeping Officers with broad legal authority to prevent and suppress offences related to (i) lèse majesté; (ii) internal security of the Kingdom; (iii) the laws on firearms; and (iv) any violation of any other orders issued by the NCPO. The order also empowers Peacekeeping Officers to issue orders prohibiting the propagation of any item of news or the sale or distribution of any book or publication or any material likely to cause public alarm to the detriment of national security or public order.

Any actions done by Peacekeeping Officers in good faith, without discrimination, in a proportionate manner, and without undue severity, shall not be subject to judicial review, either by an administrative court, civil court, or criminal court.

On April 16, 2015, NCPO Order No. 5/2558 (2015) was issued to amend Order No. 3/2558. Its provisions can be summarised as enabling additional categories and ranks of military officer to become Peacekeeping Officers.

Martial Law Act B.E. 2457 (1914) (the "MLA")
Following the imposition of martial law on Thailand in 20 May 2014, the NCPO were vested with extensive powers of government. While martial law has been revoked under Order 3/2558, it remains in force in Thailand's southern border provinces of Pattani, Yala, Narathiwat and Songkhla. In relation to surveillance and censorship of communications data specifically, the following provisions may provide the NCPO with wide powers. However, the exact manner in which such provisions may be exercised remains unclear.

Under section 10, the military authority may require from any person or company any conveyance, beast of burden, provisions, arms, instruments and tools for use in military service at that time.

Section 12 states that the military authority may, if it deems appropriate, cause provisional seizure of all things so as to prevent the enemy from using them or for the benefit of military service.

The below legislation also provides for special powers in times of national security or emergencies.

Internal Security Act B.E. 2551 (2008) (the "Internal Security Act")
Under the Internal Security Act, arrests and prosecutions must follow legal procedures. However, the definition of "threat" under the Internal Security Act is vague, and the NCPO therefore have wide discretion to determine what is and is not a "threat" and what activities to monitor. It gives officials of the Internal Security Operations Command (a unit of the Thai military dedicated to national security issues) a wide range of police powers normally exercised by civilian authorities, including powers to use both lethal and non-lethal force, to arrest and detain individuals, to conduct searches, to enter premises overtly and covertly, and to lay criminal charges.

Telecommunications Business Act B.E. 2544 (the "TBA")
Under section 63 TBA, the National Broadcasting and Telecommunications Commission is given wide powers in the event of an emergency, or where necessary to maintain public order, national security or economic stability or to protect public interests. It may take possession of and use the devices and equipment of the licensed telecommunications

provider, or authorise a state agency to temporarily take charge of a telecommunications provider's services, or order the telecommunications business or his/her employees to take a specific action until the end of such emergency or necessity.

Radio Communications Act B.E. 2544 (the "RCA")
Under section 14 RCA, for the purpose of maintaining the public order or defending the realm, the Minister of MICT is empowered to issue a provisional order to the competent authority to seize, put to use, prohibit the use of, or prohibit the removal of radio communication equipment, or part thereof, within the period and under the conditions specified in the order.

NCPO notification no. 26/2557 on supervision and surveillance on the use of online social media (the "NCPO Notification No. 26/2557")
NCPO Notification No. 26/2557 was issued on 24 May 2557 (2014). Under this notification, the permanent secretary of the ICT ministry shall establish an online social media committee which has the power to examine, inspect, and access "online information". It has broad powers to suspend or close online publications, websites and social media platforms on a number of grounds, including for engaging in incitement or agitation, for undermining the credibility or integrity of the law, or resisting or opposing the performance of the NCPO's duties. The notification does not provide any guidance as to how such powers shall be exercised by the committee.

Please note that since the abolition of martial law, the Peacekeeping Officers under Section 4(4) of Order No. 3/2558 are empowered to police any violations of this Notification.

OVERSIGHT OF THE USE OF POWERS

As, at the time of this report, Thailand is under an indefinite state of emergency, and thus the applicable oversight functions set out below may not be followed.

The expansive powers given to the authorities by the Internal Security Act, the Martial Law Act, and the NCPO Order No. 3/2558 are subject to almost no independent oversight mechanisms (save for actions which are not in good faith, discrimination, and that are not in proportion could be subject to the judicial review). The Prime Minister is required, under the Internal Security Act, to report to the parliament when the 'threat to internal security' has subsided or can be addressed within the normal powers of the government agencies.

Administrative Court Procedure Act B.E. 2542 (the "ACP")
Decisions of the National Broadcasting and Telecommunications Commission can be appealed within the organisation itself, but may also be appealed to the ACP.

An administrative case is generally initiated in the Administrative Court of First Instance, unless provisions of a specific act specifically state the dispute be filed directly at the Supreme Administrative Court.

When a dispute is to be filed at the Administrative Court, the procedure follows an inquisitorial system and any decision made by the Administrative Courts of First Instance may be appealed to the Supreme Administrative Court.

PUBLICATION OF AGGREGATE DATA RELATING TO USE OF GOVERNMENT POWERS

Restrictions on network operators and service providers
Ordinarily there is no legislation which prevents the publication of aggregate data relating to the use by the government of the powers described in this report. However under the expansive extrajudicial powers vested in the government under NCPO Order No. 3/2558 issued under Section 44 of the Interim Constitution, it has the authority to restrict publishing of any types of data which are not in the national interest.

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.

Law stated as at 16 April 2015.