Legal Annexe: Overview of legal powers

Digital Rights and Freedoms
Vodafone Group Plc

vodafone

Contents

The content covered in this Legal Annexe was updated following analysis completed in spring 2016.

Transparency and the law

This Legal Annexe is produced to accompany our transparency disclosures published within the Vodafone *Digital Rights and Freedoms Reporting Centre*.

The Annexe seeks to highlight some of the most important legal powers available to government agencies and authorities seeking to access customer communications across the 28 countries included within our Law Enforcement Disclosure Statement. While the legal powers summarised here form part of local legislation in each of these countries and can therefore be accessed by the public, in practice very few people are aware of these powers or understand the extent to which they enable agencies and authorities to compel operators to provide assistance of this nature. The contents of this Legal Annexe do not form legal advice and should not be relied upon as such. Neither Vodafone nor Hogan Lovells accepts any responsibility or liability to any person in relation to this Legal Annexe or its contents. Please see the full Disclaimer on page 5.

Creation of this Annexe

This Annexe has been compiled by our legal counsel in 28 countries with support from the international law firm, Hogan Lovells and their network of local law firms. It contains information on the meaning of some of the most important laws that empower government agencies and authorities to demand access to customer communications and to block or restrict access to communications. It also includes a new section on laws related to encryption.

Compiling this Annexe is a complex task. Vodafone counsel and the external law firms supporting us in this work have had a number of discussions about the meaning and interpretation of some of the laws that govern disclosure of aggregated demand statistics. Laws are frequently vague or unclear and there is commonly a lack of judicial guidance in interpreting the law that exists. Precise interpretation is difficult, exacerbated further (as we highlight in our Law Enforcement Disclosure Statement) by significant uncertainty on the part of some governments themselves, even when we have sought guidance from them.

During 2016, we worked with Hogan Lovells to update the existing content of this Legal Annexe for those countries of operation that had new laws in force, specifically Belgium, Czech Republic, France, Italy, Kenya, the Netherlands, New Zealand, Australia, the Democratic Republic of Congo, Greece, Romania, Spain and Turkey. It is worth noting that at the time of updating the existing content (completed in the spring of 2016) new laws were proposed or pending in several more of our countries of operation including Germany, Ghana, Hungary, Ireland, Lesotho, Malta, Mozambique, the Netherlands, South Africa, Turkey and the UK.

The additional section on encryption is intended to help inform what is now an intense public debate, as we explain in our Law Enforcement Disclosure Statement. We have chosen to cover this additional area because, as we note in our Statement, encryption is widely perceived to be an important enabler of freedom of expression, allowing individual citizens to seek and share information and opinions freely online with confidence that their communications will remain private. At the same time, the rapid spread of encrypted devices that cannot be accessed – and communications content that cannot be read – by law enforcement and intelligence agencies is a source of concern for many governments.

What this Annexe covers

In this third edition of this Legal Annexe, we focus on three key areas:

1. Laws empowering government agencies and authorities to demand access to customer communications;
2. Laws empowering government agencies and authorities to require operators to block or restrict access to communications; and
3. A new section surveying laws related to encryption in the context of law enforcement assistance in the telecommunications sector.

The legal powers summarised in these three areas are specifically relevant to our local licensed telecommunications businesses and can usually be found in telecommunications statutes or in the conditions of the licence issued by governments to those operators.

In looking at the first area, we focus on the three categories of legal power that account for the vast majority of all government agency and authority demands we receive and which are also of greatest interest in the context of the current public debate about government surveillance. Those categories are:

- lawful interception;
- access to communications data; and
- national security or emergency powers.

An explanation of each of these three categories can be found earlier in the Law Enforcement Disclosure Statement. We have also outlined some of the most common types of legal powers used to demand assistance from local licensed operators in the same section. However, we have not covered other areas, such as the many and varied 'search and seizure' powers.

In looking at the second area, we review three further categories of legal powers related to censorship that may be used by government agencies or authorities to require operators to block or restrict access to a communications network, content or services. Those categories are the:

- shut-down of network or communications services;
- blocking of access to URLs and IP addresses; and
- powers enabling government agencies and authorities to take control of a telecommunications network.

An explanation of each of these categories can also be found earlier in our Law Enforcement Disclosure Statement.

It should be noted that the legal powers described do not provide a comprehensive overview of all powers that could be used to block or restrict access to communications within our countries of operation. For example, we have not sought to catalogue court rulings ordering internet service providers or telecommunications operators to block access to certain sites or content (for example, in respect of copyright infringement or prohibited under laws outlawing obscenity).

In terms of the third area of legal powers described here, we instructed the international law firm, Hogan Lovells, and their network of local law firms (and who assisted us in preparing the Legal Annexe in 2014 and 2015) in each country to undertake a survey of the laws governing encryption in the context of law enforcement assistance in the telecommunications sector, focusing on three questions:

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?
2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?
3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and content of the communication on receipt of a lawful demand?

The survey also sought to identify examples in each jurisdiction where legislation which predated the advent of commercial encryption (which we estimate as circa 1990) had been applied to contemporary cases involving encryption.

Summary of findings on encryption

The lack of a legal framework related to encryption in many countries presented a challenge for the Vodafone local market legal teams and external law firms involved in undertaking the survey. Rather than rely on definitive legal precedents (very few of which exist), our external counsel developed a view of the legal position in each country based upon their interpretation of the wording of relevant statutes, their understanding of existing academic schools of thought and known government policy positions. This Legal Annexe should therefore be read as an informed but preliminary assessment based on a wide range of inputs.

The findings of the survey are set out in this Legal Annexe. In summary, we found that:

- in many countries, there is no legal framework related to encryption whatsoever;
- in answer to question 1, it is clear in the intent of the law in all countries (although not necessarily expressly stated) that where the telecommunications operator holds the key to an encrypted service it can be compelled to decrypt communications upon receipt of a lawful demand;
- the law is generally silent in response to questions 2 and 3 with no certainty in statute for any telecommunications operator or communications service provider regarding what is legally permissible; and
- there is extensive scope for general law enforcement legislation, national security and civil emergency powers and a wide array of other laws to be interpreted as relevant to encryption matters in a manner which cannot be predicted.

Question 2 *('Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?')* relates to a significant proportion of the data traffic carried by almost every telecommunications operator worldwide.

This can lead to some challenging situations when a law enforcement agency issues an operator with a lawful demand for access to communications data but then discovers it must approach a third party – often in a different jurisdiction – to demand the encryption key. The law in many countries does not acknowledge this complexity; indeed, the survey compiled by our external counsel found that in 10 of our 28 countries, the statutory wording could be read as placing the obligation on the operator to supply a key held by a third party – an action that in practice would be wholly unfeasible.

An increasing proportion of data traffic is encrypted end-to-end in such a way that only the sender and recipient can see the cleartext communications. This scenario is addressed in Question 3 *('Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and content of the communication on receipt of a lawful demand?')* and is also problematic from a legal perspective. The survey compiled by Hogan Lovells indicates that while no country expressly prohibits licensed telecommunications operators from providing a service with end-to-end encryption, any operator providing such a service (or considering doing so) would need to take into consideration its existing legal obligations (which may include law enforcement assistance obligations) or seek regulatory approval.

Operators are subject to national laws in the countries in which they operate and are required under national law to provide government agencies with access to private communications data upon receipt of a lawful demand. Providing unbreakable end-to-end encrypted communication services would seem, at face value, to remove an operator's ability to comply with those legal requirements. In addition, in some countries operators may be required to consult local regulators before launching such a service, in which case the answer to Question 3 remains uncertain until such time as local regulators have provided a response.

The use of general laws that predate modern technology in order to address present-day law enforcement and intelligence requirements increases the risk that a licensed telecommunications operator could face prosecution for activities that it could not reasonably have understood were proscribed at the time. We asked Hogan Lovells and their network of local law firms to form an opinion of the extent of that risk based on *'examples in each jurisdiction where legislation which predated the advent of commercial encryption (which we estimate as circa 1990) had been applied to contemporary cases involving encryption'*.

The results of the legal survey demonstrated that the use of legislation in this way was not widespread. However, the attempted application by the FBI of the All Writs Act of 1789 to compel Apple to unlock an encrypted iPhone belonging to a suspected terrorist provides an example of the scope for creative legal interpretation. A similar 'retrofitting' approach could be extended to a wide range of laws in our countries of operation, ranging from traditional police search and seizure powers and evidence preservation rules to emergency constitutional powers that come into force in the event of a national emergency such as war or mass civil unrest.

Our contribution to the debate

We would emphasise that individual countries' legislation will not always fall neatly under the categories of legal powers covered and this Annexe therefore should not be read as a comprehensive guide to all potentially relevant aspects of the law in any particular country. However, in seeking to adopt a consistent approach across 28 countries, we hope that this Annexe will serve as a useful framework for further analysis in future. As part of our commitment to informing public debate on these important topics, we continue to make this Annexe available under a Creative Commons licence and – in doing so – would encourage others to reuse and build upon our analysis in the interests of greater transparency.

The Telecommunications Industry Dialogue (TID) has highlighted our work in this area as highly beneficial for society as a whole. Other telecommunications operators have followed suit, choosing to develop country summaries for those local markets where we have no operating presence. TID has collated the country-by-country legal summaries produced by a number of those operators (including Vodafone) in one location.

Copyright licence

Disclaimer

Vodafone is grateful to Hogan Lovells for its assistance in collating the legal advice underpinning this country-by-country Legal Annexe. Hogan Lovells has acted solely as legal advisor to Vodafone. This Legal Annexe may not be relied upon as legal advice by any other person, and neither Vodafone nor Hogan Lovells accept any responsibility or liability (whether arising in tort (including negligence), contract or otherwise) to any other person in relation to this report or its contents or any reliance which any other person may place upon it.

The content covered in this Legal Annexe was updated following analysis completed in spring 2016.

Albania

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

The Interception Law

Article 22 of Law No. 9157, dated 4.12.2003 'On interception of electronic communications', as amended (the **Interception Law**), provides that when the Albanian Intelligence Agency or the relevant ministry cannot implement an interception using only their own resources, the Director of the Albanian Intelligence Agency or the relevant minister may request the assistance of any operator of electronic communications in the Republic of Albania, and the operators are bound to undertake all necessary steps in relation to such interception.

Under Article 6 of the Interception Law, the relevant organisations that have the right to require interception are: the Albanian Intelligence Agency, the Intelligence department/policy of the Ministry of Interior, Ministry of Finance and Ministry of Justice, or any other Intelligence/police service established by law. According to Articles 7–9 of the Interception Law, such request is made to the Attorney General or in his absence to any other prosecutor duly authorised by the Attorney General who will decide on the approval or rejection of the request for interception.

Under Article 21 of the Interception Law, operators of electronic communications, ie Vodafone, shall provide, at their own expense, the necessary technological infrastructure within 180 days from the issue of the request by the agencies that manage interception systems. The infrastructure for providing interception capacity shall be compatible with the equipment of the central interception point (which is the technical equipment managed by the Office of the Attorney General that allows or prevents interception of electronic communications) and the interception sector in the Albanian Intelligence Agency. If the operators of electronic communications undertake any technological change or extension in their system's capacity, they shall cover at their own expense any changes required to maintain the intercept capability. In cases of changes in the central interception point that require changes in the infrastructure of the operators of electronic communications systems, the operators are notified of such changes at least 180 days before such change takes place.

Under Article 22 of the Interception Law, the operators of electronic communications shall be provided with a copy of the decision of the Attorney General or any of his authorised persons deciding on the interception, with restricted content removed that might impair the intelligence/interception process. Such decision shall include timeframes allowing operators of electronic communications to identify numbers, addresses and other relevant data that need to be identified for the interception. When necessary, the decision is accompanied with an additional document specifying other technical details. Note that the results of interceptions acquired according to the Interception Law cannot be presented as evidence in criminal proceedings, except for data obtained in accordance with Articles 221–226 of the Criminal Procedure Code.

Criminal Procedure Code

Under Article 222 of Law No. 7905, dated 21.03.1995 'On Criminal Procedure Code', as amended (Article 208, 191/a, 208/a, 299/a, 299/b – the **Criminal Procedure Code**), upon the prosecutor's written application or that of the aggrieved party, the Court through a Decision may authorise the interception of communications. The interception is authorised when it is essential to the continuation of the initiated investigation or when there is sufficient evidence to support the charges. The relevant authorities (ie Attorney General, relevant ministries, Albanian Intelligence Agency, etc) have the capability to intercept electronic communication without the knowledge or approval of operators of electronic communications.

2. Disclosure of communications data

Electronic Communication Law

Operators of electronic communications have the duty to disclose to the competent organisations relevant communications data of their network users pursuant to the legal request of relevant public organisations made as per the procedure in accordance with the Law No. 9918, dated 19.05.2008 'On electronic communications in the Republic of Albania' (**Electronic Communication Law**), Criminal Procedure Code or the Interception Law, as the case may be.

Article 101(6) of the Electronic Communication Law provides that the relevant authorities shall be provided with any files stored in relation to their users and such files shall be made available, in electronic format as well,

Albania

without any delays to such authorities as prescribed in the Code of Penal Procedure, upon their request.

These files include data in relation to voice communication and SMS/MMS that make available the following:

a. full identification of the subscribers;
b. identification of the terminal equipment used in the communication; and
c. determination of location, date, time, duration and the outgoing/incoming number, including calls with no answer.

In cases of internet communication, the files shall include:

a. relevant data on the origin/source of communication:
   - subscriber/user ID;
   - name and address of the registered subscriber/user who owns the IP address, the identity of the user, or telephone number used during the communications;
b. relevant data on the identification of the destination/recipient of the communication:
   - in cases of internet calls, the subscriber/user ID or the telephone number of the number called;
   - in cases of email or internet calls, the name and address of the subscriber or user and the user ID of the aimed recipient of the communication;
c. relevant data for the determination of date, time and duration of the communication:
   - log-in/log-off date and time;
   - IP address, determining also if it is dynamic or static; and
   - subscriber/user ID registered for the service of internet access.

All such data shall be retained in accordance with the applicable legislation on data protection in Albania. Operators of electronic communications have the duty to disclose to the competent organisations any files stored in relation to their users and such files shall be made available, in electronic format as well, without any delays to such authorities pursuant to the legal request of relevant public organisations made as per the procedure in accordance with the Electronic Communication Law and Criminal Procedure Code.

It is not legally permitted for operators in Albania to store the content of communications as only the data provided in Article 101(6) of the Electronic Communication Law are permitted in the files stored by the operators. Therefore, only this data can be retrieved by the relevant authorities in Albania.

Data Protection Law

In addition, Article 6(2) of the Law No. 9887, dated 10.08.2008 'On Protection of Personal Data' as amended (**Data Protection Law**), provides that the processing (including transferring) of personal data in the context of prevention and/or investigation of criminal acts, for criminal acts against the public order and other criminal acts, including those in the field of national security and defence, are undertaken by the responsible authorities provided by law.

Criminal Procedure Code

Under Article 208 of the Criminal Procedure Code, the judge or the prosecutor (as the case may be, depending on the stage of investigation), based on a reasoned decision, shall decide on the seizure of material evidence relating to a criminal act when this is necessary to the confirmation of evidence. The seizure is made by the same authority issuing the decision or by any authorised police officer.

3. National security and emergency powers

Electronic Communication Law

Article 8 (rr) of the Electronic Communication Law states that it is one of the duties of the Authority on Postal and Electronic Communication (the **Authority**) to undertake any measure or order in relation to the operators of public electronic communications to implement their obligations related to the protection of the interest of the country, of the public order, and during war or extraordinary situations.

Under Article 111 of the Electronic Communication Law, operators are obliged, with their own networks and services, to face the state needs in extraordinary situations, and when requested to serve to the national defence and public order interests.

The operators providing access to the public electronic communications networks and providing electronic communications services available to the public shall develop and submit to the Authority a plan of measures to ensure the integrity of the public communications networks and to ensure access to their public communications services in extraordinary situations.

The Electronic Communication Law defines extraordinary situations as serious damages to the network, natural disasters, state of emergency or state of war. The Authority's orders oblige operators to implement emergency measures throughout the duration of the extraordinary situation. The relevant minister, in cooperation with the other agencies legally authorised to cope with extraordinary situations and with the Authority on Postal and Electronic Communication, proposes to the Council of Ministers the measures to be included in the notices issued to the operators.

Additionally, under Law No. 8756, dated 26.03.2001 'On Civil Emergencies', government authorities have the right to use any private or public means or to cooperate

Albania

with organisations related to emergency situations, in order to avoid or limit consequences from disasters in accordance with the applicable laws, as long as such circumstances exist. This provision can be interpreted as to also be extended to a range of actions towards the network of electronic communication operators in national security orders or in civil emergencies.

4. Oversight of the use of powers

Criminal Procedure Code

Under Article 222 of the Criminal Procedure Code, upon the application of the prosecutor or the aggrieved party, the Court authorises interception through a decision approving the legal interception, when it is essential to the continuation of the initiated investigation or when there is sufficient evidence to support the charges.

When there are reasonable doubts that any delays may impair the investigations, the prosecutor decides on the interception and issues an approval and informs the Court immediately, in any case not later than 24 hours. Within 48 hours from the decision of the prosecutor, the Court makes an assessment of the prosecutor's decision. If such assessment is not made within these time limits, the interception cannot continue and its results cannot be used. The Interception Law also provides for cases of interceptions authorised through a Court decision always based on the relevant articles of the Criminal Procedure Code (Articles 221–226). Article 212 of the Criminal Procedure Code provides that the defendant or the person against whom a seizure is sought or the person who filed the criminal suit are entitled to appeal against such Decision of the Court.

Under Article 23 of the Interception Law, the Attorney General or the prosecutor duly authorised by him provides for and communicates to the operator of electronic communications the decision of the relevant Court on the interception.

Operators of electronic communication are bound in principle by this duty of technological assistance and capability adjustment/adaptation related to interception (Article 21 of the Interception Law) pursuant to a request by the relevant organisations managing interception systems in accordance with the Interception Law.

Censorship-related powers

1. Shut-down of network and services

Albanian Constitution

Article 170 of the Albanian Constitution provides for certain extraordinary measures which the government may legally take under the conditions of war, natural disasters or other type of extraordinary situation in order to address such an emergency. Under this provision, it would therefore be possible for parliament to approve a specific law requiring the shut-down or taking control of a communication service provider's network or services (such as Vodafone's) for as long as the extraordinary situation, war or natural disaster existed.

Law No. 8756

Under Law No. 8756, where there is a civil emergency, government authorities may work with network operators (such as Vodafone) to avoid or limit the consequences arising from the civil emergency. A civil emergency is any major event that immediately and gravely endangers human life, cultural heritage or wealth, or the environment – such as a major ecological disaster, mass industrial action, social unrest (for example, riots), terrorist attack or war. The government authorities may use any private or public means, or cooperate with organisations, to resolve the situation, but must do so in accordance with applicable law. While the exact measures and powers are not described, according to this law, Vodafone is obliged to organise, when it is deemed necessary, the evacuation of their employees from their facilities and cooperate with the government to make available their services in response to an emergency situation in the area of the civil emergency. It may be feasible that in specific cases such cooperation between a network operator (such as Vodafone) and the government could extend to the shutting down of Vodafone's network or services for as long as the civil emergency existed.

Electronic Communication Law

Under Article 76 of the Electronic Communication Law, the Authority on Postal and Electronic Communication has the right to revoke the authorisation of a network operator (such as Vodafone) to use the radio frequencies on which it operates its network. The Authority may only do so in specific circumstances.

Such circumstances include where the Authority identifies that the network operator's licence application contained false data or the network operator has infringed provisions of the Electronic Communication Law or conditions of its authorisation (including payment of licence fees). The Authority may also remove the network operator's licence if the network operator has not used the specified frequencies for one year or has used them for a different purpose to that authorised. Regardless of the network operator's behaviour, the Authority may also revoke authorisation to use certain radio frequencies if doing so is the only means by which to avoid harmful radio interference.

The impact of revoking Vodafone's authorisation to use some or all of its radio frequencies would have the practical effect of shutting down part or all of its network or services, depending on the extent of the revocation.

Albania

Under Article 111 of the Electronic Communication Law, Vodafone is obliged to withstand with its own network and services the state needs on extraordinary situations and national protection of security and public order. Based on this article, the government may propose different measures for addressing extraordinary situations related to the national protection of security and public order, which may include the government taking control of or shutting down a network operator's network and services.

Under Article 134, the Authority on Postal and Electronic Communication may order that the equipment of a network operator be confiscated or that the network operator be banned from using it, if the network operator violates the law or causes harmful interferences to the network. The practical impact of this would be the shutting down of part or all of the network operator's network or services.

2. Blocking of URLs and IP addresses

The Authority on Postal and Electronic Communication may notify network operators to block access to certain URLs, IP addresses and/or IP ranges if requested to do so by a public or regulatory authority. Most commonly, this would be the prosecutor's office, a judicial court or any other public institution that is given by the law competences to make such decisions.

In late 2013, following the approach of the Albanian Government against gambling, the Supervisory Unit of Gambling liaised with the Authority on Postal and Electronic Communication and ordered all mobile operators and ISPs to block access on their networks to any website providing offshore online gambling services. Since then, offshore gambling websites have been blocked by network operators in Albania.

3. Power to take control of Vodafone's network

Electronic Communication Law

Please see 'Shut-down of network and services' above. Under Article 111, the government's powers may extend to taking control of a network operator's network and services, for as long as the extraordinary situation related to national protection of security and public order shall last.

Law No. 8561

This Law provides the Albanian Government (acting through central or local government authorities) with the right to temporarily take control of private property where to do so is in the public interest and such public interest cannot otherwise be protected. Under Article 27, such public interest includes where there is an extraordinary event (the meaning of which is outlined in Section 1 'Shut-down of network and services' above) or war. Government use of private property cannot extend past the legal reason for which it was established and, in any event, for no more than two years. It is feasible that these powers could allow a government authority to take control of Vodafone's network.

A request by the government to take control of private property must include a description of the property that will be taken control of; the reason and term of the control; and an offer of compensation to the owner of the property. Under Article 34, in exceptional and urgent cases when the circumstances do not allow any delay, the government authority may take immediate control of the property. However, within 24 hours the government authority must present a request for endorsement under Law No. 8561. Where private property is taken over by central government, such activity must be authorised by the relevant government minister.

4. Oversight of the use of powers

Electronic Communication Law

Under Article 136 of the Electronic Communication Law, decisions relating to the confiscation of equipment by the Authority can be appealed to the courts. Other decisions of the Authority are subject to the Administrative Procedure Code. The Code is a law that provides all the rules applied and used by all public institutions. Typically, according to the Code, any decision of a public institution can be subject to court proceedings only after all the administrative appeal steps (ie appeal before the superior authority of the administrative institution concerned) have been exhausted, unless the Code provides otherwise and allows direct appeal to the courts.

Law No. 8561

Under Article 37 of Law No. 8561, the owner of the property being taken control of by the government authority has the right to appeal to the courts against that decision. The property owner may also appeal the level of compensation offered or the specific conditions of the property use. Such appeal must be made within 30 days. Therefore, Vodafone could choose to appeal to the courts were a government authority to take control of its network.

Albania

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes. The relevant legislation is the Criminal Code and the Interception Law, both of which are referred to at the beginning of this country section.

As addressed earlier in this country section, Article 22 of the Interception Law provides that when the authorities fail to implement the lawful interception, they may request the assistance of the operator; the latter is then bound to undertake all necessary steps in relation to such interception.

In addition, the Criminal Procedure Code (Article 208/a para 2), despite being a technologically updated provision, seems to impose a catch-all obligation to disclose data stored/held with the electronic communications operators.

Under these circumstances and having the obligation to enable/assist successful interception and disclose communications data, we conclude that the provision of decryption keys of such communications data in cases when the operator is in possession of the decryption key is mandatory by law.

Article 101(6) refers only to the traffic communications data and location data (otherwise known as call details records or relevant metadata) and does not cover the communication data that can be stored or held with the operator.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

No. There is no explicit provision in the Interception Law that obliges operators to support decryption of communication on third party services. On the contrary, Article 21/1 of the Interception Law stipulates that operators should build the necessary infrastructure to ensure interception capability over their users/customers, which make use of the operators' own electronic communication services.

In addition, under Article 3 of the Interception Law, only operators who are locally licensed/authorised to conduct telecommunication activity are subject to the Interception Law, which means that any third party which is not licensed/authorised by a local regulatory body would not be subject to interception rules. It is therefore our implicit understanding that the duty to provide interception lies with a licensed operator's own services/networks . Practically speaking, this means that in order for a law enforcement agency to capture all communication data in their country, all operators in that country would need to be licensed and bound by the interception rules.

Based on the above, decryption of third party communication data by a telecommunications operator could be interpreted as unlawful interception and a breach of communication privacy/secrecy law under the Constitution and the Interception Law.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and content of the communication on receipt of a lawful demand?

There is not any express mandatory law provision that limits a telecommunications operator in providing end-to-end encryption on its communication services.

Nevertheless, from the perspective of interception obligations under the Interception Law, a telecommunications operator must offer, at its own expense, the technological solutions that would enable the competent authorities to perform the interception activity whenever it is required to do so. The issue with end-to-end encryption is that it makes it impossible to commit to decrypt the communications when and if requested.

Based on the above and acknowledging that end-to-end encryption limits a telecommunications operator's capacity to comply with the lawful interception obligations, we conclude that in practical terms a telecommunications operator cannot offer end-to-end encryption because it would not be capable of decrypting such communication should the authorities request to intercept it at a later stage.

4. Please provide examples in your jurisdiction where legislation that predated the advent of commercial encryption (which we estimate as circa 1990) has been applied to contemporary cases involving encryption.

There are no such precedents in Albania.

Australia

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Australia is a federation containing three separate types of legislation: Commonwealth, state and territory. This report focuses on the legal powers available to the Australian government and law enforcement agencies under commonwealth law.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

Telecommunications Act 1997

Carriers and carriage service providers (carriers), such as Vodafone, have legislative obligations under the Telecommunications Act 1997 (**TA**) to provide assistance to law enforcement agencies and national security agencies with the interception of individual customer communications (live communications) where authorised.

Section 313(3) of the TA requires carriers to give officers and authorities of the Commonwealth such help as is reasonably necessary for the purposes of: (i) enforcing the criminal law and laws imposing pecuniary penalties; (ii) assisting the enforcement of the criminal laws in force in a foreign country; (iii) protecting the public revenue; and (iv) safeguarding national security. Section 313(7) of the TA specifies that a reference to 'giving help' under section 313(3) of the TA includes the provision of interception services, including services in executing an interception warrant under the Telecommunications (Interception and Access) Act 1979, and the providing of relevant information about any communication that is lawfully intercepted under an interception warrant (sections 313(7)(a) and 313(7)(c)(i) of the TA).

Section 313(1) of the TA requires a carrier to do its best to prevent telecommunication networks and facilities from being used in, or in relation to, the commission of offences against the laws of the Commonwealth or the States and Territories. Examples of the kind of help law enforcement and national security agencies might request under section 313(3) of the TA include: (i) the provision of interception services; (ii) information from a carrier's information base, such as billing records; and (iii) assistance in tracing a call.

Under Part 16 of the TA, a carrier may be required to supply a carriage service for defence purposes or for the management of natural disasters.

Telecommunications (Interception and Access) Act 1979

The Telecommunications (Interception and Access) Act 1979 (the TIA Act) gives law enforcement agencies and national security agencies the power to intercept live communications in specified circumstances.

Under Chapter 2 of the TIA Act, interception warrants may be issued in respect of live communications to the Australian Security Intelligence Organisation (ASIO) and certain state and federal law enforcement agencies. Interception warrants permit such agencies to intercept telecommunications for national security, in emergencies and for law enforcement purposes.

Interception warrants may be issued by the Federal Attorney General to the Director-General of Security, or an ASIO employee or affiliate appointed by the Director-General of Security under sections 9 and 9A of the TIA Act for security purposes. Under section 10 of the TIA Act, the Director-General of Security can issue an interception warrant in certain specified emergencies where the Attorney General cannot issue the warrant in sufficient time. Under sections 11A, 11B and 11C of the TIA Act, telecommunications service warrants, named person warrants and foreign communications warrants, for the collection of foreign intelligence, may be issued to the Director General of Security or an ASIO employee or affiliate appointed by the Director General of Security. A named person warrant issued under section 11B may authorise entry on any premises specified in the warrant for the purpose of installing, maintaining, using or recovering any equipment used to intercept foreign communications (section 11B(1B) of the TIA Act). Under section 11C(4)(a), a foreign

Australia

communications warrant must include a notice addressed to the carrier who operates the telecommunications system giving a description identifying the part of the telecommunications system that is covered by the warrant.

Under section 30 of the TIA Act, the interception of live communications may occur (without a warrant being issued) by the police in specified urgent situations; for example, where there is risk to loss of life or the infliction of serious personal injury or where threats to kill or seriously injure another person have been made. The police are able to request a carrier to intercept individual communications in these circumstances for the purposes of tracing the location of a caller. (Part 23 of Chapter 2 of the TIA Act).

Interception of live communications may also be authorised (without a warrant) under section 31A of the TIA Act by the Attorney General to enable security authorities for the purpose of developing and testing interception capabilities (Part 24 of Chapter 2 of the TIA Act).

Under Part 2-5 of Chapter 2 of the TIA Act, interception warrants may be issued to agencies that are defined as interception agencies, which in turn are defined as Commonwealth agencies or an eligible agency of a State in relation to which a declaration under section 34 of the TIA Act is in force. These agencies could include the Australian Federal Police (AFP), the Australian Crime Commission, the Independent Commission Against Corruption and the State Police Forces. Interception warrants are issued by an 'eligible judge', namely a judge of a court created by the Commonwealth Parliament who has consented to being nominated, or by nominated members of the Administrative Appeals Tribunal (AAT) (sections 46 and 46A of the TIA Act). Interception warrants may only be issued in relation to the investigation of serious offences as defined in section 5D of the TIA Act.

Parts 5-2 to 5-5 of Chapter 5 of the TIA Act impose obligations on carriers to ensure that it is possible to execute a warrant issued for interception purposes, unless an exemption has been granted. Specific technical capabilities are imposed, including, by way of example, the nomination of delivery points in respect of a particular kind of telecommunication service of a carrier (section 188). In practice, when served with a warrant, the carrier will be required to intercept all traffic transmitted, or caused to be transmitted to and from the identifier of the target service used by the interception subject and described on the face of the warrant. The carrier will also need to deliver the intercepted communications through an agreed delivery point from which the intercepting agency may access those communications.

Under Part 5-3 of Chapter 5 of the TIA Act, the minister may make determinations in relation to interception capabilities applicable to a specified kind of telecommunication service that involves, or will involve, the use of the telecommunication system. Carriers and nominated carriage service providers may be required under such determinations to lodge annual Interception Capability Plans (IC plan) with the Communications Access Co-ordinator of the Attorney General's Department. Part 5-4 of Chapter 5 of the TIA Act specifies the obligations of a carrier in relation to an IC plan such as the matters to be set out in an IC plan (section 195(2)) and the time for delivering IC plans (sections 196 and 197).

Under Part 5-5 of Chapter 5 of the TIA Act, the Communications Access Co-ordinator may make determinations in relation to delivery capabilities applicable to specified kinds of telecommunications services, and to one or more specified interception agencies relating to such matters as the format in which lawfully intercepted information is to be delivered to an interception agency, the place and manner in which such information is to be delivered, and any ancillary information that should accompany that information.

The Australian Security Intelligence Organisation Act 1979

While the Australian Security Intelligence Organisation Act 1979 (ASIO Act) enables ASIO to use listening devices under warrants issued by the Minister (section 26 of the ASIO Act), this section, or a warrant issued under this section, does not apply or relate to the use of a listening device for a purpose that would, under the TIA Act, constitute the interception of a communication passing over a telecommunications system operated by a carrier.

A computer access warrant may be issued under the ASIO Act and may allow the use of a telecommunications facility operated by a carrier for the purpose of obtaining access to data that is relevant to a security matter and is held in the target computer at any time while the warrant is in force (section 25A of the ASIO Act).

Australia

The Crimes Act 1914

The Crimes Act 1914 (Cth) (**Crimes Act**) authorises certain officers of the AFP and State and Territory police to obtain information pursuant to search warrants issued under the Crimes Act from premises, computers or computer systems and information in relation to telephone accounts held by a person. The Crimes Act does not only apply to carriers.

Section 3LA of the Crimes Act enables a constable (a member or special member of the AFP or a member of the police force or police service of a state or territory) to apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to enable a constable to access data held in, or that is accessible from, a computer or data storage device.

Under section 3ZQN of the Crimes Act, an authorised AFP officer may give a person a written notice requiring that person to produce documents that relate to serious terrorism offences.

Under section 3ZQO of the Crimes Act, an authorised AFP officer may apply to a judge of the Federal Circuit Court of Australia for a notice requiring a person to disclose documents relating to serious offences. Such documents may relate to a telephone account held by a specified person and details relating to the account, such as the details in respect of calls made to, or from, the relevant telephone number.

2. Disclosure of communications data

Disclosure of stored communications

Telecommunications (Interception and Access) Act 1979

Under Part 3-1A of the TIA Act, certain agencies are allowed to give preservation notices to carriers to preserve stored communications that the carrier holds that relate to a person or particular telecommunications service. There are broadly two types of preservation notices: domestic preservation notices (which can be either historic or ongoing and which relate to stored communications that might relate to contraventions of certain Australian laws or to security); and foreign preservation notices (which relate to stored communications that might relate to contraventions of certain foreign laws). The purpose of these preservation notices is to prevent stored communications being destroyed before a warrant has been issued to access these stored communications.

Part 3 of the TIA Act enables ASIO and specified government agencies to access stored communications pursuant to a stored communication warrant issued under the TIA Act for the purpose of national security and law enforcement.

Under Part 3-3 of Chapter 3 of the TIA Act, stored communication warrants for law enforcement purposes may be issued to criminal law enforcement agencies for the purpose of investigating serious contraventions. Such agencies include but are not limited to agencies such as the ACCC, the Australian Securities and Investments Commission (ASIC) and the Independent Commission Against Corruption. ASIO can access stored communications using its existing interception warrants (section 109 of the TIA Act).

Stored communication warrants can be issued by certain nominated judges and nominated AAT members in relation to the investigation of serious contraventions. Serious contraventions, by way of example, include an offence under a law of the Commonwealth, a state or a territory that is punishable by imprisonment for a maximum period of at least three years. Stored communication warrants may also be issued as part of a statutory civil proceedings that would render the person of interest to a pecuniary penalty.

The Crimes Act 1914

Under the Crimes Act, an authorised AFP officer may access metadata or stored communications pursuant to a search warrant.

The Australian Security Intelligence Organisation Act 1979

Under section 25A of the ASIO Act a stored communication may be accessed under a computer access warrant issued to ASIO. Additionally, a stored communication can be accessed by ASIO if the access results from, or is incidental to, action taken by an officer of ASIO, in the lawful performance of his or her duties, for the purpose of: (i) discovering whether a listening device is being used at, or in relation to, a particular place; or (ii) determining the location of a listening device (see section 108(2)(f) and (g) of the TIA Act).

Disclosure of telecommunications data

Chapter 4 of the TIA Act specifies the circumstances in which telecommunications data may be voluntarily disclosed to government and law enforcement agencies by carriers or carriage service providers and the conditions by which authorisations can be issued requiring the disclosure of information.

Telecommunications data is not defined in the TIA Act but is well understood to mean the metadata relating to communications, but not the contents or substance of communications themselves.

Sections 174 and 175 of the TIA Act provide for the disclosure of information to ASIO. Information may be disclosed voluntarily if it is in connection with the performance of ASIO's functions. Information may otherwise be disclosed pursuant to an authorisation issued by the Director General of Security, the Deputy Director General of Security or a specified employee or affiliate of ASIO. Authorisations may be in respect of existing information or prospective information (specified information or documents that

Australia

come into existence during the period for which the authorisation is in force).

Sections 177 to 180 of the TIA Act specify the circumstances in which disclosure of information or a document may be made to an enforcement agency. Voluntary disclosure of information may occur if the disclosure is reasonably necessary for the enforcement of the criminal law. Disclosure of information may also occur pursuant to authorisations issued by an authorised officer of an enforcement agency for the purpose of:
(i) the enforcement of the criminal law;
(ii) the location of missing persons; and
(iii) the enforcement of a law imposing a pecuniary penalty and for the protection of the public revenue.

Sections 180A to 180E of the TIA Act specify the circumstances in which disclosure of specified information or specified documents may be made to an officer of the AFP, or authorised by an authorised officer of the AFP, for the enforcement of the criminal law of a foreign country.

On 13 October 2015, the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (DR Act) came into force. The DR Act amended the TIA Act and introduced a requirement for network operators to retain and secure specific telecommunications data for a period of two years for each communications service they provide.

Under the new Part 5-1A, an obligation was introduced for carriers to retain certain specified data for two years from the date on which the information or document is created. Carriers must keep certain types of subscriber information throughout the life of the account and for a further two years after closure of the relevant account.

The DR Act permitted network operators to apply for a time extension during which they would be exempt from complying with the requirements of the DR Act applying from 13 October 2015 through the lodging of a Data Retention Implementation Plan (DRIP) and approval of this DRIP by the Communications Access Co-ordinator. This process was introduced to allow network operators additional time to implement a fully compliant data retention system.

The DR Act limited data access to an approved list of agencies that have operational or investigative need to access the retained metadata. However, existing state and territory-based laws continue to allow access to a wide range of agencies and bodies in those states and territories. Law enforcement and security agencies will continue to make requests for access to telecommunications data as previously.

Telecommunications Act 1997

Carriers have legislative obligations under the TA to provide assistance to law enforcement and national security agencies, including an obligation to disclose information where authorised.

Under section 284 of the TA, disclosure of information to the ACMA, the Australian Competition and Consumer Commission (ACCC), the Telecommunications Ombudsman or the Children's e-Safety Commissioner is permitted where the information may assist those agencies to carry out their functions.

Sections 279 and 280 of the TA permit the disclosure of information if the information is used in the performance of a person's duties as an employee of a carrier or where the disclosure is authorised under a warrant and by law.

Section 313(7) of the TA specifies that a reference to giving help under section 313 of the Act includes giving effect to a stored communications warrant and to providing relevant information about any communication that is lawfully accessed under a stored communications warrant (sections 313(7)(b) and 313(7)(c)(ii)).

The Crimes Act 1914

Under the Crimes Act, an authorised AFP officer may access metadata or stored communications pursuant to a search warrant.

3. National security and emergency powers

Telecommunications Act 1997

The TA enables the Secretary of the Defence Department of the Chief of Defence Force to require the supply of a carriage service for defence purposes or for the management of natural disasters.

Under section 335 of the TA, a Defence authority may give a carriage service provider a written notice requiring the provider to supply a specified carriage service for the use of the Defence Department or the Defence Force. If a requirement is in force, the provider must supply the carriage service in accordance with the requirement, and on such terms and conditions as are agreed between the provider and the Defence authority or, failing agreement, determined by an arbitrator appointed by the parties.

Division 4 of Part 16 of the TA provides that a carrier licence condition may include a 'designated disaster plan' for coping with disasters and/or civil emergencies prepared by the Commonwealth, a state or a territory.

Australia

4. Oversight of the use of powers

Telecommunications (Interception and Access) Act 1979

The TIA Act contains a number of safeguards and controls in relation to interception and access to stored communications and telecommunications data as well as a number of reporting requirements. These requirements are designed to ensure that appropriate levels of accountability exist.

Under the TIA Act, records relating to interception warrants and the use, decimation and destruction of intercepted information must be maintained by law enforcement authorities. The Commonwealth Ombudsman is required to inspect certain records (such as those maintained by the AFP) and report to the Minister (Part 2-7 of Chapter 2 of the TIA Act).

Part 2-10 of Chapter 2 of the TIA Act provides that a person who was a party to a communication, or on whose behalf a communication was made, can apply for a civil remedy to the Federal Court of Australia or a court of a state or territory if that communication was intercepted in contravention of the Act. Section 7(1) of the TIA Act prohibits the interception of a communication passing over a telecommunication system except in specified circumstances, for example where conducted under a warrant or by an officer of ASIO. Division 6 of Part 4-1 of Chapter 4 of the TIA Act creates offences for certain disclosures and uses of information and documents. By way of example, it is an offence to disclose information concerning whether an authorisation has been sought and the making of an authorisation unless disclosure is reasonably necessary to enable law enforcement agencies to enforce the criminal law.

Section 186 of the TIA Act requires an enforcement agency to give the minister a written report, no later than three months after 30 June, of all authorisations issued under Chapter 4 of the TIA Act in the preceding financial year. The Minister must then prepare a summary report of all reports received under section 186(1) and cause a copy of that report to be tabled before Parliament.

Similar reporting requirements are placed on criminal-law enforcement agencies and the minister in respect of stored communication warrants as in relation to interception warrants (Part 3-6 of Chapter 3 of the TIA Act). Part 3-7 of Chapter 3 of the TIA Act provides that an aggrieved person can apply for a civil remedy to the Federal Court of Australia or a court of a state or territory in relation to an accessed communication, if information relating to it is disclosed in contravention of section 108 of the TIA Act.

Under Chapter 4A of the TIA Act, the Commonwealth Ombudsman must inspect records of an enforcement agency to determine compliance with Chapter 4 of the TIA Act. This Chapter sets out the powers of inspection and powers of the Commonwealth Ombudsman to request information from agencies.

Telecommunications Act 1997

Section 314 of the TA provides that, when providing help to an officer or authority of the Commonwealth, a state or a territory under section 313(3) or (4), a party (carrier) must comply with the requirement to help on such terms and conditions as are agreed between the party and relevant agency or, failing agreement, as determined by an arbitrator appointed by the parties. Where the parties fail to agree on the appointment of an arbitrator, the ACMA is to appoint the arbitrator.

Judicial review

Judicial review of government decision-making by a court is available under sections 39B(1) and 39B(1A) of the Judiciary Act 1903 (Cth) and section 75(v) of the Constitution. For example, in relation to the decision by a government officer to issue a warrant.

Section 39B(1) confers jurisdiction on the Federal Court with respect to any matter in which a writ of mandamus (that is, an order requiring a public official to perform a duty or exercise a statutory discretionary power), certiorari (that is, an order quashing an act), prohibition (that is, an order preventing someone from performing a specified act), or an injunction (a Court order requiring a person to do, or refrain from doing, a certain thing) is sought against an officer of the Commonwealth.

Section 39B(1A) provides that the Federal Court's original jurisdiction also includes jurisdiction in any matter 'arising under any laws made by the Parliament' (other than a criminal matter).

Under section 75(v) of the Constitution, the High Court (Australia's highest court) has original jurisdiction in all matters in which a writ of mandamus or prohibition or an injunction is sought against an officer of the Commonwealth.

Judicial review does not concern itself with the merits of a decision, but considers whether a decision-maker has made their decision within the limits of the powers conferred by statute, the Constitution and the common law. So, when reviewing a decision to issue an interception warrant, the Court will examine the legislation under which access to the data was granted and whether the requirements for granting access were met.

Australia

Censorship-related powers

1. Shut-down of network and services

The government does not have the legal authority to require the shutdown of Vodafone's entire network for censorship related purposes. However, the police can request the shutdown of an individual's mobile service in limited circumstances.

Telecommunications Act 1997

Under Section 315 of the TA a police officer, not below the rank of Assistant Commissioner, may request a network provider (such as Vodafone) to suspend the supply of a mobile service in the case of an emergency. The police officer may only make such a request of Vodafone if he or she has reasonable grounds to believe that: (i) an individual has done (or has imminently threatened to do) an act that has resulted in, or is likely to result in, loss of life or serious personal injury, or the individual has made an imminent threat to cause serious damage to property or do an act that is likely to endanger their health or safety; (ii) the individual has access to Vodafone's mobile service; and (iii) the suspension is reasonably necessary to prevent or reduce the likelihood of those acts occurring (or, as the case may be, recurring).

2. Blocking of URLs and IP addresses

Telecommunications Act 1997

Regulatory bodies and law enforcement agencies can require network providers (such as Vodafone) to provide assistance necessary to enforce the law including by requesting the blocking of IP addresses and/or ranges of IP addresses under Section 313 of the TA. The Australian Federal Police have put in place a section 313 request to require Vodafone to block access to Interpol's 'worst of' list of websites containing child sexual abuse images.

Broadcasting Services Act 1992

Under Schedule 5 and Schedule 7 of the Broadcasting Services Act 1992, the Australian Communications and Media Authority (ACMA) is empowered to require internet service providers (such as Vodafone) to take action in respect of websites where they contain prohibited content. Content is prohibited where it is, or in ACMA's judgment is likely to be, a refused classification or classified X18+; classified R18+ and not protected by a restricted access system. Where the content is hosted within Australia, the ACMA may require removal of the content, the link or service, or require the use of a restricted access system (see Schedule 7, clauses 47, 56 and 62 of the Broadcasting Services Act 1992). Where the prohibited content is hosted outside of Australia, the blocking is carried out by use of filtering software that internet service providers are required to offer to their customers; the software works by referring to a list of banned websites (and their URLs) maintained by ACMA (see Schedule 5, clause 40(1)(b) of the Broadcasting Services Act 1992 and clause 19 of the Internet Industry Codes of Practice – Internet and Mobile Content 2005). ACMA also has the power to issue local websites with a 'take-down' notice in respect of content that must be removed (see Schedule 5, clause 47 of the Broadcasting Services Act 1992); the step of blocking the website's URL usually follows when the requested take-down has not occurred.

3. Power to take control of Vodafone's network

The government does not have legal authority to take control of Vodafone's network.

4. Oversight of the use of powers

Judicial review

Under Section 75(v) of the Australian Constitution, the High Court has original jurisdiction in all matters in which a writ of mandamus, prohibition or injunction is sought against an officer of the Commonwealth.

At a lower level in the court hierarchy, the Federal Court has original jurisdiction over any matter arising under any laws made by Australia's parliament, except for a criminal matter pursuant to Section 39B(1A). Under Section 39B(1), the Federal Court can decide on any matter in which a writ of mandamus, certiorari, prohibition or an injunction is sought against an officer of the Commonwealth.

Judicial review does not concern itself with the merits of a decision, but considers whether a decision-maker has made their decision within the limits of the powers conferred by Australia's Constitution, statute and common law.

Australia

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

The following legislative provisions are relevant to this question.

Telecommunications Act 1997

Under section 313(3) of the TA, telecommunications operators must provide such help to agencies (for example, law enforcement agencies) as is 'reasonably necessary' for enforcing the criminal law and laws imposing pecuniary penalties, protecting public revenue and safeguarding national security.

The reference to giving help in section 313(3) includes giving help by way of:

a. the provision of interception services, including services in executing an interception warrant under the Telecommunications (Interception and Access) Act 1979;

b. giving effect to a stored communications warrant under that Act;

c. providing relevant information about:
   - any communication that is lawfully intercepted under such an interception warrant; or
   - any communication that is lawfully accessed under such a stored communications warrant;

(ca) complying with a domestic preservation notice or a foreign preservation notice that is in force under Part 3-1A of that Act; giving effect to authorisations under Division 3 or 4 of Part 4-1 of that Act; or

d. giving effect to authorisations under Division 3 or 4 of Part 4-1 of that Act; or

e. disclosing information or a document in accordance with section 280 of this Act.

If a telecommunications operator has encrypted data and content, holds the encryption key and therefore has the technological ability to 'unlock' that data and content, we consider the requirements of Section 313(3) would extend to include a requirement to decrypt the data in circumstances where the required legal grounds for interception, access or disclosure are satisfied.

Telecommunications (Interception and Access) Act 1979

As set out in the interception and disclosure country annexe for Australia, the TIA Act gives law enforcement agencies and national security agencies the power to intercept live communications in specified circumstances. Part 3 of the TIA Act enables ASIO and specified government agencies to access stored communications pursuant to a stored communication warrant issued under the TIA Act for the purpose of national security and law enforcement. Chapter 4 of the TIA Act specifies the circumstances in which telecommunications data may be voluntarily disclosed to government and law enforcement agencies by carriers or carriage service providers and the conditions by which authorisations can be issued requiring the disclosure of information.

As is the case with Section 313(3) of the TA, our view is that the obligations under each of these provisions of the TIA Act extend to require telecommunications operators to decrypt content where they hold the encryption key in order to give full effect to the rights of the relevant agencies under the legislation.

Under the new Part 5-1A of the TIA Act, an obligation was introduced for carriers to retain certain specified data for two years from the date on which the information or document is created. Carriers must keep certain types of subscriber information for a longer period: throughout the life of the account and for a further two years after closure of the relevant account. Under section 187BA of the TIA Act introduced through the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (the DR Act), the carrier is expressly required to protect the confidentiality of information that it must keep under section 187A of the TIA Act by encrypting the information and protecting the information from unauthorised interference or unauthorised access.

The Explanatory Memorandum to the DR Act indicates that where a service provider encrypts retained data, the service provider must retain the technical capability to decrypt and disclose relevant retained data in a usable form in accordance with a lawful request under the TIA Act or the TA.

We note that there is no applicable case law on these issues and this answer is therefore based on statute.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

The government has no specific, express legal authority to require telecommunications operators to decrypt data carried on its networks as part of a telecommunications service where the encryption has been applied by a third party.

Australia

We do not consider that the requirement to give agencies 'help' under section 313(3) of the TA will extend to decrypting third party OTT or user-encrypted data that was not encrypted by a telecommunications operator and where the operator does not hold the encryption key. Decrypting, or attempting to decrypt, third party OTT or user-encrypted data would place financial and resource obligations on a telecommunications operator that we do not think are envisaged by the statute. In addition, decrypting or attempting to decrypt this data without the knowledge or consent of these third parties could, in some circumstances, lead to legal recourse against the telecommunications operator.

There are no provisions in the TIA Act that would extend to requiring a telecommunications operator to seek to decrypt such traffic. In the case of Part 5-1A (which relates to the retention of telecommunications data), there is an express provision that states that the carrier is not required to retain any information that is carried by means of another service (ie an OTT service).

We note that there is no applicable case law on these issues and this answer is therefore based on statute.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

No, a telecommunications operator would not be able to offer end-to-end encryption that it does not have the technological capacity to breach without breaching its existing law enforcement obligations.

Under Part 5-4 of the TIA Act, telecommunications operators are required to provide an interception capability plan to the Communications Access Co-ordinator (a function of the Attorney General's Department) each year on or around 1 July. The interception capability plan must set out the strategies for compliance with an operator's legal obligation to provide interception capabilities and a statement of the compliance by the operator with that legal obligation.

In addition, section 202B of Part 5-4A of the TIA Act requires telecommunications operators to notify the Communications Access Co-ordinator of any change to a service or system that is likely to have a material adverse effect on the capacity of it to comply with its obligations under the TIA Act or Section 313 of the TA (more particularly described in the answer to Question 1 above). The Communications Access Co-ordinator then has a period of 30 days to notify the operator that it must not implement the change.

In this scenario, we consider it highly likely that the Communications Access Co-ordinator would reject a proposal to implement end-to-end encryption that an operator does not have the capacity to break. That is because such implementation would have a material adverse effect on the ability of relevant agencies to intercept communications.

It is likely that the implementation of such a service would be treated as non-compliance with Section 313 of the TA. Finally, Section 106 of the TIA Act also provides that a person must not obstruct or hinder a person acting under a warrant. It is possible that this provision could be breached in circumstances where an operator unilaterally implements an end-to-end encryption service that it does not have the capacity to break. That is because such action would have the effect of preventing an agency from exercising the warrant.

We note that there is no applicable case law on these issues and this answer is therefore based on statute.

4. Please provide examples in your jurisdiction where legislation that predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

We are not aware of any legislation in Australia that predates the advent of commercial encryption used to produce judgments that are then applied to use of commercial encryption.

Belgium

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

Code of Criminal Procedure

The Code of Criminal Procedure makes it possible to impose measures with a view to intercepting a person's communications following a warrant by the examining magistrate (*juge d'instruction/ onderzoeksrechter*). This warrant also needs to be communicated to the public prosecutor.

A warrant is an order coming from the examining magistrate in which he or she imposes special investigation measures, including interception measures. This order needs to explain why such measures are needed and under which circumstances they will be used.

Article 90ter of the Code of Criminal Procedure grants the examining magistrate, under specified circumstances and for specific cases, the power to issue real-time interception measures.

Article 90quater, Section 1 of the Code of Criminal Procedure states that the warrant issued by the examining magistrate and authorising the interception measure needs to be signed and needs to contain:

i. the indications and the concrete facts proper to the case justifying the interception measure(s);
ii. the reasons for which the measure is necessary to reveal the truth;
iii. the person, means of communication/ telecommunications and/or the place of surveillance;
iv. the period during which the surveillance can be executed (no longer than one month starting from the decision ordering the measure); and
v. the name of the criminal police officer that has been designated to execute the measure.

Article 90quater, Section 2 of the Code of Criminal Procedure states that if the interception measure implicates some kind of processing of a communications network, the operator of this network or provider of a telecommunications service ('electronic communications operator') needs to cooperate, if the examining magistrate in person or through a police service requests so.

The Royal Decree 2003

The Royal Decree of 9 January 2003 on the modalities for the legal 'cooperation duty' in the case of legal action relating to electronic communications lays out the details of this cooperation duty. Article 6 of the Royal Decree deals with the ability for electronic communication operators to assist in real-time interception operations.

The Royal Decree on legal cooperation duty following legal actions states that every electronic communications operator needs to designate one or more persons being charged with the cooperation duty (ie the duty to cooperate with the prosecution and investigation authorities with a view to tracking down/identifying/intercepting certain data). These persons form the so-called 'Coordination Cell Justice'. Electronic communications operators can decide to form a shared Coordination Cell. This Cell takes the measures which are necessary for interception of private communications or telecommunications following receipt of the warrant of the examining magistrate.

The Intelligence and Safety Services Act 1998

The Intelligence and Safety Services Act of 30 November 1998 states that intelligence and safety services are allowed to intercept a person's communications, if national security is at stake. This interception can only be executed after a written request from the Director-General of the State Security ('the Director-General').

A real-time interception is a so-called 'exceptional method for collecting data'. These exceptional methods need to be authorised by the Director-General. With regard to the exceptional methods, Article 18/10 of the Intelligence and Safety Services Act of 30 November 1998 describes the authorisation to be granted by the Director-General prior to the execution of the interception measures. Before this authorisation becomes final, it has to be made subject to the advice of the Administrative Commission supervising the specific and exceptional methods for collecting data by the intelligence and safety services ('the Commission'). The advice of the Commission determines whether the relevant legislation and general principles of subsidiarity and proportionality have been respected. If the advice is negative, the interception measure cannot be executed.

Belgium

The authorisation needs to be in writing and contain:

i. a description of the exceptional threats justifying the interception;
ii. the reasons why the interception is necessary;
iii. the names of persons or entities whose communications are being intercepted;
iv. the technical means used to intercept;
v. the period of interception; and
vi. the names of the intelligence officers involved in the operation.

With regard to an interception measure (in addition to the Article 18/10 authorisation), Article 18/17, Section 1 of the Intelligence and Safety Services Act of 30 November 1998 states that the intelligence services can intercept a person's communications. Section 3 states that electronic communications operators are required to cooperate with the intelligence services if the interception requires processing by an electronic communications network.

As mentioned above, the Director-General needs to draft a written request to the relevant operator in order for the latter to cooperate. This request contains the advice of the Commission on the general authorisation to use interception measures (as laid down in Article 18/10).

The Royal Decree 2010

The Royal Decree of 12 October 2010 on specific rules for the legal 'cooperation duty' in case of actions of the intelligence services regarding electronic communications lays out the details of this cooperation duty. Every electronic communications operator needs to designate one or more persons being charged with the cooperation duty (ie the duty to cooperate with the intelligence services authorities with a view to tracking down/identifying/intercepting certain data). These persons form the so-called ' Coordination Cell Justice'. Electronic communications operators can decide to form a shared Coordination Cell. This Cell takes the measures which are necessary to intercept private communications or telecommunications following the receipt of the written and reasoned decision of the Director-General of the intelligence services.

The Electronic Communications Act 2005

Article125, Section 2 of the Electronic Communications Act of 13 June 2005 (relating to interception demands coming from authorities competent in prosecution and investigation of criminal offences and/or the intelligence services), states that the King determines the modalities on the means to be put in place in order to identify, track down, localise, become aware of and intercept electronic communications. These modalities have been determined in the Royal Decree of 15 October 2010 mentioned above.

Article 127, Section 1, 2° of the Electronic Communications Act lays out the technical and administrative measures electronic communications operators need to take in order to be able to identify, track down, intercept and become aware of private communications (on demand of competent authorities and/or the intelligence services). If they do not take such measures (ie internal procedures for dealing with these requests), they are not allowed to offer the electronic communications service in respect of such measures.

2. Disclosure of communications data

The Electronic Communications Act 2005

The Electronic Communications Act of 13 June 2005 contains provisions for the duty of electronic communications operators to provide metadata on demand from the competent prosecution/investigation authorities (see below – Criminal Procedure Code) and from the intelligence services (see below – Intelligence and Safety Services Act of 30 November 1998):

Article 122, Section 1 of the Electronic Communications Act of 13 June 2005 states that electronic communications operators may be required not to remove or to anonymise traffic data relating to subscribers or end users, if authorities prosecuting criminal offences or the intelligence services require them to do so.

Article 125, Section 2 states that the King determines the modalities on the means to be put in place with a view to identifying, tracking down, localising, becoming aware of and intercepting electronic communications.

Article 127, Section 1, 2° lays out the technical and administrative measures electronic communications operators need to take with a view to being able to identify, track down, intercept and become aware of private communications. If they do not take such measures (ie internal procedures for dealing with these requests), they are not allowed to offer the electronic communication services for such measures. The modalities on these measures have been determined in the Royal Decree on legal cooperation duty following legal actions, mentioned below.

The Royal Decrees of 2003 and 2010

Article 6, Section 1, 1° of the Royal Decree on legal cooperation duty following legal actions and Article 8, Section 1, 1° of the Royal Decree on cooperation duty following intelligence service actions specify that the content of communications may be transmitted to the authorities prosecuting and investigating criminal offences as well as the intelligence services.

Belgium

The requirements of the Electronic Communications Act as described above should also be borne in mind when considering the following criminal procedures and intelligence services-related procedures.

The Criminal Procedure Code

There are specific authorisations and notifications required for investigation measures set out under the Criminal Procedure Code:

- Article 46 bis: Following a reasoned written decision from the public prosecutor, an electronic communications operator may be required to provide data allowing a subscriber/user of an electronic communications service or an electronic communications service to be identified.
- Article 88 bis: Following a reasoned court order from the examining magistrate, he or she may require, directly or through a police service, an electronic communications operator to provide data allowing the identification and location of a subscriber or an electronic communications service.

For every means of telecommunication used and subject to a court order, the day, hour, duration and location of the call are recorded in an official report (*proces-verbaal/procès-verbal*).

The Intelligence and Safety Services Act 1998

Collection of identification and localisation data relating to a subscriber or end-user is classified as a specific method of investigation (whereas interception measures are considered to be exceptional methods).

Article 18/3 of the Intelligence and Safety Services Act of 30 November 1998 states that identification and localisation data can only be disclosed after a written and reasoned decision by the Director-General and after notification of this decision to the Administrative Commission supervising the specific and exceptional methods for collecting data by the intelligence and safety services.

Article 18/7, Section 1 of the Intelligence and Safety Services Act of 30 November 1998 states that the electronic communications operators have to provide data allowing the identification and/or localisation of a subscriber to or user of an electronic communications service as well as data relating to the means and ways of payment of the subscription fees and/or user fees of an electronic communication service. (The Director-General needs to address a written decision to the operators in order to obtain their cooperation, in addition to the Article 18/3 decision.)

Article 18/8, Section 1 of the Intelligence and Safety Services Act of 30 November 1998 states that the electronic communications operators have to provide data allowing the tracking of call identification data and locating the origin or the destination of the means of electronic communication.

The Royal Decree on cooperation duty following intelligence service actions, mentioned above, lays out the details of these requirements, ie that this communication of data needs to be done by the Coordination Cell of Justice.

3. National security orders and emergency powers

Electronic Communications Act 2005

Under Article 4 of the Electronic Communications Act, the King can fully or partially prohibit the provision of electronic communication services in the interests of public security (after consultation with the Council of Ministers).

Civil Contingencies Act 2007

Under the Civil Contingencies Act of 15 May 2007, the government is given broad powers for a limited period of time during civil emergencies, which could in theory extend to a range of actions in relation to Vodafone's network and/or customers' communications data in Belgium.

For instance, Article 181 of the Civil Contingencies Act states that the Ministers competent for internal affairs and for health, or their delegates, may seize everyone and/or everything in the framework of interventions for missions of civil contingency (rescue missions, etc), if there are no public services available. In theory, this could also include the communications data and/or network of Vodafone.

4. Oversight of the use of powers

With regard to the interception measure ordered by the examining magistrate pursuant to the Criminal Code Procedure, the persons whose communications have been intercepted can argue that the interception was illegal. They can do this before a pre-trial chamber (*Chambre du conseil/Raadkamer*) during the pre-sentence stage (before the case is treated on its merits). They can also do this during the treatment of the case on its merits before the Criminal Court, before the Court of Appeal or eventually before the Court of Cassation.

With regard to the interception executed by the Intelligence and Safety Services Act of 30 November 1998, there is administrative oversight. Article 18/10, Section 6 of this Act states that, at any time, the members of the Commission can exercise control over the legality of the measures (including the principles of proportionality and subsidiarity).

Belgium

In order to exercise this control, they can go to places where the intercepted data are received or registered. They can request all useful documents and they can interrogate members of the intelligence services. If the Commission concludes that the threat(s) at the origin of the interception measure no longer exist(s) or that the interception measure is no longer useful, it ends the measure (or suspends it in case of illegalities).

If the Commission concludes that the data are being obtained under illegal conditions, they are kept under the supervision of the Commission (after advice from another Commission, ie the Commission on the protection of the privacy ('Privacy Commission')). The Commission prohibits the use of the illegally obtained data and suspends the measure if it is still in place.

Pursuant to Article 43/2 of the Intelligence and Safety Services Act of 30 November 1998, the so-called '*Vast Comité I/Comité Permanent R*' (Vast Comité I) is charged with a posteriori control over the interception measures (ie reviewing the legality and respect for the principles of proportionality and subsidiarity of the decisions in order to execute the interception measures and of the methods used). If the Vast Comité I concludes that the measure is illegal, it orders all data obtained through the measure to be destroyed and prohibits any exploitation of these data. There is no appeal possible against the decisions of the Vast Comité I.

Regarding the disclosure of communications data, pursuant to the Criminal Code Procedure, the persons whose communications data have been disclosed can argue that the disclosure was illegal. They can do this before the pre-trial chamber (*Chambre du conseil/Raadkamer*), during the pre-sentence stage (before the case is treated on its merits). They can also do this during the treatment of the case on its merits, before the Criminal Court, before the Court of Appeal or, eventually, before the Court of Cassation.

With regard to the disclosure of metadata executed by the Intelligence and Safety Services Act of 30 November 1998, there is administrative oversight. Pursuant to Article 18/3, Section 2 at the end of every month, a list of executed measures (including the disclosure measures) is sent to the Commission. At any time, the members of the Commission can exercise control over the lawfulness of the measures (including the principles of proportionality and subsidiarity). In order to exercise this control, they can go to those places where the disclosed data are received or registered. They can request all useful documents and they can interrogate members of the intelligence service. If the Commission concludes that the data is being obtained under unlawful conditions, such data may be kept under the supervision of the Commission after advice is taken from the Commission on the Protection of Privacy ('Privacy Commission'). The Commission prohibits the use of illegally obtained data and suspends the measures if they still are in place.

Under the Electronic Communications Act 2005, any Royal Decree can be challenged before the Council of State. The Council of State can then decide to confirm or repeal the Royal Decree.

There is no judicial oversight of the use of powers under the Civil Contingencies Act 2007.

Censorship-related powers

1. Shut-down of network and services

Electronic Communications Act

Under Article 4 of the Electronic Communications Act, the King of Belgium can fully or partially prohibit the provision of electronic communication services in the interests of public security after consultation within Belgium's Council of Ministers. Such a Royal Decree could order the shut-down of Vodafone's entire network or some of its services.

2. Blocking of URLs and IP addresses

The government does not have any legal authority to order Vodafone to block specified URLs and/or IP addresses.

However, the judge can order Vodafone to block IP addresses and/or ranges of IP addresses, if it appears that illegal material is being transmitted through the IP addresses it manages.

Chapter VI of Book XII of the Economic Law Code – the Law of the Electronic Economy – states that the competent judicial authorities may require internet service providers to terminate or prevent certain infringements consisting of the transmission of illegal material.

3. Power to take control of Vodafone's network

The government does not have legal authority to take control of Vodafone's network.

Belgium

4. Oversight of the use of powers

Electronic Communications Act

Any Royal Decree by the King can be challenged before the Council of State. The Council of State can then decide to confirm or repeal the Royal Decree.

Book XII, 'The Law of the Electronic Economy', of the Economic Law Code

Any court order with a view to requiring internet service providers to terminate or prevent certain infringements consisting of the transmission of illegal material will be subject to classical judicial oversight at the time of the request. If made, a court order may be subject to an appeal before the Court of Appeal. The judgment of the Court of Appeal may be subject to a further appeal before the Court of Cassation.

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes, under specific circumstances.

Article 8, Section 1, 4° of the Royal Decree on cooperation duty following intelligence service actions and Article 6, Section 1, 4° of the Royal Decree on legal cooperation duty following legal actions state that in communicating data to the competent prosecution/investigation authorities or the intelligence agency, in the framework of surveillance measures, the content of the communication needs to be comprehensive. If the operators have encrypted or encoded certain data, they need to lift this encryption/code.

Article 127, Section 2 of the Electronic Communications Act prohibits any provision or use of a service or equipment hindering the execution of the measure which operators need to take to communicate certain data to the competent authorities, unless the encryption systems are being used to guarantee the confidentiality of the communication and the safety of payments (this prohibition is not applicable to electronic communication services provided on the basis of a prepaid card (this will change in the near future)).

Under Article 90quater, Section 4 of the Criminal Procedure Code, the examining magistrate can oblige competent persons to decrypt encrypted data, in order to obtain access to the content of the concerned data.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

Under Article 90quater, Section 4 of the Criminal Procedure Code, the examining magistrate can oblige competent persons to decrypt intercepted encrypted data, in order to obtain access to the content of the concerned data.

More particularly, any person whom the examining magistrate estimates has particular knowledge of the telecommunications service subject to surveillance or of the services allowing the encryption of registered data can be ordered by the examining magistrate to provide information on how to decrypt the concerned information in such a way that its content is accessible to the examining magistrate.

The examining magistrate can order persons to make accessible the content of an intercepted telecommunication in the way he or she wants it to be accessible. The persons who have been given the order have to do so, as far as they are capable of doing so.

In other words, if the examining magistrate estimates that a telecommunications operator is capable of decrypting certain data carried on its network, he or she can order the telecommunications operator to decrypt that data or, at least, to provide assistance with a view to decrypting the data, even if the encryption has been applied by a third party.

Article 88quater, Sections 1 and 2 of the Criminal Procedure Code, contains the same rules regarding obtaining access to computer systems that are subject to a search ordered by the examining magistrate.

Belgium

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

As a principle under Belgian law, the use of encryption is free (this is stated under Article 48 of the Electronic Communications Act).

However, Article 127, Section 2 of the Electronic Communications Act prohibits any provision or use of a service or equipment hindering the execution of the measure which operators need to take to communicate certain data to the competent authorities, unless the encryption systems are being used to guarantee the confidentiality of the communication and the safety of payments.

In other words, as long as the telecommunications operator can demonstrate that the encryption software it offers does not aim to hinder the communication of data to the competent authorities, but aims to guarantee the confidentiality of the data and/or the safety of payments, the provision of encryption software is not contrary to its existing law enforcement obligations (the reasoning is the same for BAU and OTT services).

In practice, there are very few limits on the use of encryption techniques in Belgium.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

We have not found examples where legislation predating the advent of commercial encryption has been used to demand access to data protected by encryption.

Czech Republic

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

Electronic Communications Act

Section 97(1) of Act No. 127/2005 Coll. on Electronic Communications (the **Electronic Communications Act**) states that a network provider is obliged on request to set up and secure an interface to enable the following authorities to carry out surveillance and recording of end telecommunication devices:

a. the Police of the Czech Republic for the purposes set out in Section 88 of the Act No. 141/1961 Coll., the Criminal Procedure Code (the **Criminal Procedure Code**);
b. the Security Information Service (*Bezpečnostní informační služba*) for the purposes set out in Sections 6–8a of the Act No. 154/1994 Coll., on the Security Information Service (the **Security Information Service Act**); and
c. the Military Intelligence (*Vojenské zpravodajství*) for the purposes set out in Sections 9–10 of the Act No. 289/2005 Coll., on Military Intelligence (the **Military Intelligence Act**).

There is no obligation imposed on the providers to directly intercept the communications.

The above authorities must show evidence of their authorisation to conduct the surveillance and recording by presenting a written request to the service provider which:

i. includes the file number under which the court decision is administered by the respective authority; and
ii. is signed by the person liable for the conduct of surveillance and recording at the respective authority.

If the request is made by the Police of the Czech Republic, it must include the file number under which the subject's consent to surveillance is administered (if applicable).

The technical requirements for connecting with end telecommunication devices are prescribed by the Decree No. 336/2005 Coll. (the **Information Decree**). This sets out the form and extent of information provided from the database of the publicly available telephone service subscribers and on the technical and operating conditions, and connection points, of the message interception and recording terminal equipment.

Police of the Czech Republic

Under Section 88 of the Criminal Procedure Code, the Police of the Czech Republic may only conduct surveillance and recording on the basis of an order for the surveillance and recording of a telecommunication operation. This order is issued by the competent chairman of the senate or a judge provided that the following conditions are met:

a. a criminal proceeding is underway for one of the crimes listed in the Criminal Procedure Code;
b. it can be reasonably presumed that the surveillance and recording will obtain important facts for the criminal proceedings; and
c. this aim cannot be achieved by different means, or would be substantially more difficult to achieve by different means.

The above order (which is a special type of judicial decision) must be issued by:

i. the chairman of the senate of the competent court; or
ii. the judge of the competent court within the preparatory proceedings, on the basis of a motion from the state prosecutor.

For certain crimes listed in the Criminal Procedure Code, surveillance and recording can be conducted without such an order, provided that the user of the respective device consents to the surveillance.

Security Information Service

The authorisation of the Security Information Service to request that an interface be set up and/or secured is regulated by Section 8a of the Security Information Service Act.

Under Section 9(1) of the Security Information Service Act, the Security Information Service may only conduct surveillance and recording:

i. with the prior written approval of the chairman of the senate of the competent high court; and
ii. provided that the discovery or documentation of activities by any other means would be ineffective, substantially difficult or impossible.

Czech Republic

Military Intelligence

The authorisation of Military Intelligence to request that an interface be set up and/or secured is regulated by Section 9(5) of the Military Intelligence Act.

Under Section 9(1) of the Military Intelligence Act, the Military Intelligence may only conduct surveillance and recording:

i. with the prior written approval of the chairman of the senate of the competent high court; and

ii. provided that the discovery or documentation of activities by any other means would be ineffective, substantially difficult or impossible.

2. Disclosure of communications data

Electronic Communications Act

Under Section 97(3) of the Electronic Communications Act, a legal entity providing a public communications network or a publicly available electronic communications service (such as Vodafone) is obliged to store traffic and location data for a period of six months and is obliged to disclose such data (including metadata) to the following authorities on request:

a. the police bodies taking part in criminal proceedings, for the purposes and under the conditions prescribed by Section 88a of the Criminal Procedure Code;

b. the Police of the Czech Republic for the purposes listed in the Electronic Communications Act (such as preventing terrorism) and under the conditions prescribed by Section 66(3) of the Act No. 273/2008 Coll., on the Police of the Czech Republic (the **Police Act**);

c. the Security Information Service for the purposes and under the conditions prescribed by Section 8a of the Security Information Service Act;

d. the Military Intelligence for the purposes and under the conditions prescribed by Section 9 of the Military Intelligence Act; and

e. the Czech National Bank for the purposes and under the conditions prescribed by Section 8 of the Act No. 15/1998 Coll., on Supervision over the Capital Market (the **Supervision Act**).

The traffic and location data (including metadata) shall be provided to the authorities listed above in the manner described in particular by Section 3 of the Decree No. 357/2012 Coll., on the preservation, transfer and deletion of traffic and location data.

Police taking part in criminal proceedings

Under Section 88a of the Criminal Procedure Code, the police bodies (as defined in Section 12 of the Criminal Procedure Code) may only request traffic and location data on the basis of an order for the provision of such data. This order is issued by the competent chairman of the senate or a judge provided that the following conditions are met:

a. a criminal proceeding is underway for one of the crimes listed in the Criminal Procedure Code; and

b. this aim cannot be achieved by different means, or would be substantially more difficult to achieve by different means.

The above order (which is a special type of judicial decision) must be issued by:

i. the chairman of the senate of the competent court; or

ii. the judge of the competent court within the preparatory proceedings, on the basis of a motion from the state prosecutor.

The traffic and location data can be requested without such an order, provided that the user of the respective device consents to the provision of the data.

Police of the Czech Republic

In relation to the form and extent of the data, Section 66(3) of the Police Act refers to Section 97 of the Electronic Communications Act.

Security Information Service

In relation to the form and extent of the data, Section 8a of the Security Information Service Act refers to Section 97 of the Electronic Communications Act.

Military Intelligence

In relation to the form and extent of the data, Section 9 of the Military Intelligence Act refers to Section 97 of the Electronic Communications Act.

Czech National Bank

In relation to the form and extent of the data which the Czech National Bank may demand, Section 8(1d) of the Supervision Act refers to Section 97 of the Electronic Communications Act and prescribes further conditions for the request of the traffic and location data, including the prior written approval of the chairman of the senate of the competent high court.

The government and law enforcement agencies in the Czech Republic do not appear to have any specific intercept powers in order to compel Vodafone to disclose the content of stored communications.

3. National security and emergency powers

Electronic Communications Act

Under Section 97(5) of the Electronic Communications Act, a provider of a publicly available telephone service is obliged to provide the Police of the Czech Republic and the General Inspection of the Security Forces on request with information from its database of participants, to the extent and in the form prescribed by the Information Decree.

Czech Republic

Under Section 99 of the Electronic Communications Act, a legal entity providing a public communications network or a publicly available electronic communications service (such as Vodafone) is entitled to provide priority access to the network for emergency communication participants (ie Ministries and other authorities) on the basis of a request from the Ministry of the Interior. The provider is entitled to restrict or interrupt the provision of publicly available telephone services for this purpose.
The provider is obliged to inform the Czech Telecommunication Office of the restriction or interruption. The restriction or interruption must not last any longer than necessary, and access to emergency numbers must be maintained.

Police Act

The authorisation of the Police of the Czech Republic and the General Inspection of the Security Forces is regulated by Section 35(3) of the Act No. 341/2011 Coll., on the **General Inspection of the Security Forces and Section 66(2) of the Police Act**.

Moreover, under Section 39(1) of the Police Act, the police force has the right to interfere with the operation of electronic communication devices, the network and the provision of electronic communications services in the event of a threat to human lives, health or property with a value exceeding CZK 5 million. This typically includes situations where there is a threat of terrorism.

The police are obliged to inform the integrated rescue system information point, the Czech Telecommunication Office, and as necessary, the operator (provided that informing the operator will not jeopardise the police force's fulfilment of its duties).

Act No. 222/1999

Finally, Act No. 222/1999 Coll., on Securing the Defence of the Czech Republic imposes further duties on legal entities and natural persons which can be requested by the Ministry of Defence and other authorities in order to ensure national security. However, this Act does not regulate any specific duties from communication service providers.

The request is filed through the competent contact points of the Police of the Czech Republic.

Act No. 239/2000

Moreover, under Section 18 of the Act No. 239/2000 Coll., on the Integrated Rescue System, providers of communication services are obliged to cooperate with the Ministry of the Interior on the preparation and resolution of emergency communications and European unified emergency numbers.

Crisis Management Act

The Act No. 240/2000 Coll., on Crisis Management (the **Crisis Management Act**) imposes further duties on legal entities and people conducting business in case of emergency. In particular, these subjects are obliged to cooperate on request in the preparation of the emergency plan (ie a plan which includes a list of emergency measures and procedures for emergency situations) and fulfil the duties prescribed in it. Moreover, legal entities and people can also be required to perform duties above and beyond the duties prescribed by the emergency plan. The Crisis Management Act does not regulate any specific duties from communication service providers.

A legal entity providing a public communications network or a publicly available electronic communication service has a statutory obligation to provide the above assistance.

4. Oversight of the use of powers

Criminal Procedure Code

Under Section 88(3) of the Criminal Procedure Code, the police bodies must continuously evaluate whether the issuance of a surveillance and recording order is still justified. If the grounds no longer exist, the police bodies are obliged to immediately cease surveillance and recording, and notify the chairman of the senate or the competent judge who issued the order. Moreover, the state prosecutor may supervise the activities of the Police of the Czech Republic (including surveillance and recording).

Security Information Service Act

Under Section 11 of the Security Information Service Act, the competent judge is authorised to request information from the Security Information Service for the purpose of considering whether the use of surveillance and recording is still justified. The judge will cancel the approval if he or she concludes that this is not the case.

Military Intelligence Act

Under Section 11 of the Military Intelligence Act, the competent judge is authorised to request information from the Military Intelligence for the purpose of considering whether the use of surveillance and recording is still justified. The judge will cancel the approval if he or she concludes that this is not the case.

In addition, the activities of all of the authorities listed in this report are supervised by special supervision bodies comprising members of the Chamber of Deputies.

Czech Republic

Censorship-related powers

1. Shut-down of network and services

Crisis Management Act

Under present law, there are currently no specific regulations which would enable the Czech government to shut down Vodafone's network or services. Theoretically, any provider's network could be shut down in responding to a crisis under the general principles of Act No. 240/2000 Coll. on Crisis Management, but this is considered highly unlikely.

Act on Cyber Security

Under Act No. 181/2014 Coll. on the Cyber Security, which became valid on 1 January 2015, the Czech National Security Authority ('NSA') is entitled to issue decisions on reactive measures to address cyber security incidents or secure information systems or networks and electronic communication services from cyber security incidents. The Act on Cyber Security provides the NSA with wide-ranging authority and it may impose an obligation on Vodafone to shut down its network as necessary.

2. Blocking of URLs and IP addresses

Criminal Procedure Code

Vodafone could be asked to block specific IP addresses or ranges of IP addresses under Section 8(1) of the Criminal Procedure Code. Under Section 8(1) all legal entities are generally obliged to assist the police in tackling criminal matters. The police may therefore request an internet service provider (such as Vodafone) to block websites featuring illegal content. However, in practice, the police do not request this type of assistance from internet service providers.

Act on Cyber Security

Under Act No. 181/2014 Coll. on Cyber Security, the NSA is entitled, inter alia, to impose an obligation on Vodafone to block URLs and/or IP addresses if reacting to a cyber-security incident.

3. Power to take control of Vodafone's network

The government does not have legal authority to take control of Vodafone's network.

4. Oversight of the use of powers

Crisis Management Act

There is no judicial oversight of the government's powers under the Crisis Management Act.

Act on Cyber Security

The Act on Cyber Security does not include any special regulation and therefore decisions of the NSA are subject to judicial review.

Criminal Procedure Code

A police request to an internet service provider to block certain IP addresses may be reviewed by the state prosecutor. This can be at the state prosecutor's request; at the request of the internet service provider subject to the order; or at the request of another party to the criminal proceedings.

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes. The relevant law is the Electronic Communications Act and the Information Decree which are defined earlier in this chapter (see 'Provision of real-time interception assistance').

Under Section 97 (6) of the Electronic Communications Act, if a legal entity providing a public communications network or a publicly available electronic communications service (hereinafter referred to as the 'CSP') implements encoding, compression, encryption or other technologies that make the transferred data unintelligible, it is obliged to ensure that the communication and related traffic and location data are intelligible at the end point for the access of the telecommunication devices of authorised authorities.

Moreover, Section 8 (4) of the Information Decree, on the form and extent of information provided from the database of the publicly available telephone service subscribers and on the technical and operating conditions, and connection points, of the message interception and recording terminal equipment (the 'Information Decree'), stipulates that if a part of the network or service is encrypted or encoded by the CSP, the content of the messages shall be provided from the part of the network or service where there is no such modification.

Czech Republic

If the whole network or service is provably encrypted or encoded and the CSP provably does not hold the encryption key, the content of the messages shall be provided in the available form. Therefore, if the telecommunications operator as a CSP holds the encryption key (ie when the communication is encrypted by the CSP), it may be required by the authorities to decrypt the communication data.

The Electronic Communications Act applies to both 'business as usual' communication services (where the communication routes over the network as a data packet) and 'over the top' communication services (where the delivery of the communication is made via Internet Protocol (IP) over the network), provided that the 'over the top' services are publicly available, ie that no user is excluded from using it beforehand.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

No. As already stated above, Section 8 (4) of the Information Decree stipulates that if the whole network or service is encrypted or encoded and the CSP probably does not hold the encryption key, the content of the messages shall be provided in the available form.

Therefore, the telecommunications operator as a CSP can be forced to decrypt communication data only if it holds the encryption key to do so. There is no obligation for the CSP to employ any other decrypting technologies other than the encryption key in order to decrypt the communication.

The statutory law on law enforcement does not contain any provisions dealing with encryption. With regard to the form in which the communication data should be disclosed, it refers to the Electronic Communications Act. There is no relevant case law relating to the interpretation of these provisions.

The Electronic Communications Act applies to both 'business as usual' communication services (where the communication routes over the network as a data packet) and 'over the top' communication services (where the delivery of the communication is made via Internet Protocol (IP) over the network) provided that the 'over the top' services are publicly available, ie that no user is excluded from using it beforehand.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

Under Section 97 (6) of the Electronic Communications Act, if a CSP implements encoding, compression, encryption or other technologies that make the transferred data unintelligible, it is obliged to ensure that the communication and related traffic and location data are intelligible at the end point for the access of the telecommunication devices of authorised authorities.

If a CSP fails to comply with this provision, it commits an administrative offence and faces relevant charges as set out under Section 118 of the Electronic Communications Act.

Should a CSP offer end-to-end encryption, it could not comply with its duties to ensure the intelligibility of the communication and related traffic and location data. Therefore, this is not an option.

The Electronic Communications Act applies to both 'business as usual' communication services (where the communication routes over the network as a data packet) and 'over the top' communication services (where the delivery of the communication is made via Internet Protocol (IP) over the network) provided that the 'over the top' services are publicly available, ie that no user is excluded from using it beforehand.

The statutory law on law enforcement does not contain any provisions dealing with encryption. With regard to the form in which the communication data should be disclosed, it refers to the Electronic Communications Act.

There is no relevant case law relating to the interpretation of these provisions.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

No such legislation was used for these purposes in the Czech Republic.

Democratic Republic of Congo

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

Framework Law No. 013-2002 on telecommunications

Articles 54(a) and 55 of the Framework Law No. 013-2002 of 16 October 2002 on telecommunications in the Democratic Republic of Congo (DRC) (**Framework Law**) provides for the interception of communications in two scenarios: firstly in the context of judicial cases where an authorisation has been granted by the Attorney General of the Republic ('Attorney General'); and secondly interceptions authorised by the Minister of the Interior in relation to national security, protection of the essential elements of the scientific, economic and cultural potential of the country, or the prevention of crime and organised crime.

Article 54(a) of the Framework Law prohibits the interception, phone-tapping, recording, transcription and disclosure of correspondence issued by telecommunications without prior permission of the Attorney General. Article 55 of the Framework Law stipulates that for the purpose of providing evidence in a court of law, it is necessary for the Attorney General to order the interception, recording and transcription of correspondence transmitted through telecommunications.

Article 59 of the Framework Law requires that interceptions authorised by the Minister of the Interior must have a purpose to:

i. seek information relating to national security;
ii. protect the essential elements of the cultural, scientific or economic potential of the DRC; or
iii. prevent crime and organised crime.

2. Disclosure of communications data

Article 13 of the Standard Licence for the provision of mobile communications services based on GSM technology provides that each telecommunication company shall submit information on a monthly basis to the Authority for Regulation concerning:

- the number of subscribers at the end of each month;
- the average call time;
- the total number of billing items;
- the number of calls from mobile telephones to fixed-line telephones, and from fixed-line telephones to mobile telephones;
- the disconnection rate;
- the BSC-number dynamics;
- the quantity and RF channel number via BTS; and
- the BTS number dynamics.

The Framework Law

Article 52 of the Framework Law provides that the secrecy of correspondence transmitted through communications is guaranteed by law in the DRC. The confidentiality of correspondence can only be lifted in cases where it is strictly in the public interest as provided by the law.

Article 53 of the Framework Law reinforces this by stating that the public operator of telecommunications and other telecommunications service providers and members of their staff are required to respect the secrecy of customers' communications.

Article 4 of Law No. 014-2002 creating the Regulatory Authority for Post and Telecommunications of Congo, (**ARPTC Law**) states that the Regulatory Authority can conduct site visits, conduct investigations and studies, and collect all the necessary data required for this purpose.

Democratic Republic of Congo

3. National security and emergency powers

The Framework Law gives the government powers to requisition telecommunications facilities for reasons of public security.

Paragraph 3 of Article 46 of the Framework Law stipulates that any employees of telecommunications facilities that are requisitioned may be required to provide their services to the competent authority.

For the purpose of public security or defence of the national territory or in the interest of the public service of telecommunications, the State may prohibit all or part of the use of telecommunications during a period that it may determine.

If Article 46 is not complied with, then the Decree Law No. 1-61 of 25 February 1961 regarding measures of state security, right of search, internment and surveillance together with its accompanying Ministerial Order 05/02 of 22 April 1961 can be applied. Article 4 of this Decree Law establishing measures of state security, right of search, detention and surveillance (**Decree Law on the National Security**) specifies that any violence or act likely to prevent or impede the search pursuant to the provisions of the Decree shall constitute a presumption of guilt.

These powers are reserved for use in exceptional circumstances, such as emergencies.

4. Oversight of the use of powers

The authorisation of the Attorney General applies for a maximum period of six months unless renewed. The authorising decision for interception by the Attorney General should include the reasoning for the use of interception, the offence leading to the use of the interception and its duration (Article 56 of the Framework Law).

This authorisation of the Minister of the Interior shall be given in writing and by justifiable decision. The authorisation must be proposed by the Minister of Defence and security or by the Head of the Intelligence Services (Article 60 of the Framework Law).

Any breach of Article 52 of the Framework Law constitutes an offence in respect to Criminal Code in the DRC.

Censorship-related powers

1. Shut-down of network and services

Telecommunications Framework Law No. 013/2002

Article 46 of the Telecommunications Framework Law No. 013/2002 provides that the State may prohibit the use of telecommunication facilities (such as Vodacom's network), in full or in part, for any period of time, as it deems fit, in the interests of public security or national defence, the public telecommunications service, or for any other reason.

This power was used to require all mobile network operators to shut down SMS service in the Democratic Republic of Congo during the period 2–28 December 2011. The same happened on 19 January 2015, when the authorities shut down internet and SMS service for mobile phones throughout the country after nationwide demonstrations led to deadly clashes with police.

More generally, under Articles 42 and 50, the government may revoke (temporarily or permanently) the licence of a telecommunications operator (such as Vodacom) if the operator does not comply with the conditions of its licence; does not comply with the legislation in force; or refuses to grant access to its network facilities to officers of the Criminal Investigation Department (who are responsible for investigating breaches of the law) when such access is requested. Under Article 43, the government may also withdraw an operator's licence if the telecommunications operator becomes wholly owned by foreign nationals. If the government were to withdraw Vodacom's licence, this would, in effect, shut down Vodacom's network.

Democratic Republic of Congo

Ministerial Decree No. 003/CAB/MIN/PTT/K/2000

In addition, Ministerial Decree No. 003/CAB/MIN/PTT/K/2000 dated 31 January 2000 allows the Ministry of Telecommunications to suspend the services of the network operator (in full or in part) pursuant to the order of a public authority. If needed, the public authorities and, in particular, the Ministry of Defence can 'requisition the network' without giving rise to any claim for compensation. This Ministerial Decree is superseded by the Telecommunications Framework Law No. 013/2002.

However, it is considered relevant to licences issued before the passing of the Telecoms Framework Law No. 013/2002.

Constitutional powers

Article 85 of the Constitution provides that the President of the Republic may declare a state of emergency or state of war when circumstances threaten seriously and immediately the independence or the integrity of the national territory, or when they cause the interruption of the normal functioning of institutions. The President may only do so after consultation with the Prime Minister and the presidents of the two Parliament chambers. Such a declaration is done by Decree and will last for 30 days' duration, which may be extended by the Parliament for successive periods of 15 days. Certain additional powers are enabled during such a period which may extend to ordering the shut-down of a network such as Vodacom's. However, in practice, Article 46 of the Telecommunications Framework Law No. 013/2002 is more likely to be relied upon, given the breadth and strength of its powers.

2. Blocking of URLs and IP addresses

Telecommunications Framework Law No. 013/2002

Given the nature of the powers provided under Article 46 of the Telecommunications Framework Law No. 013/2002 – in particular those described directly below under 'Power to take control of Vodacom's network', it is feasible that the government might order, or implement, the blocking of URLs and IP addresses on Vodacom's network.

3. Power to take control of Vodacom's network

Telecommunications Framework Law No. 013/2002

With the powers provided for under Article 46 of the Telecommunications Framework Law No. 013/2002 (please see above under 'Shut-down of network and services'), the State may also requisition (or order its officials to requisition) telecommunication facilities. In such instances, the personnel normally working at these facilities may be required to provide their services to the competent authority, if so requested. This could, in effect, mean that the government could take control of Vodacom's network, requiring Vodacom staff to operate the network on its behalf.

4. Oversight of the use of powers

Telecommunications Framework Law No. 013/2002

There are a posteriori (after the event) possibilities for judicial oversight and the annulment of illegal use of powers with respect to the Telecommunications Framework Law 2002.

The Supreme Court may be seized of an action for annulment for excess use of power in respect of any administrative decisions issued by central government authorities on the grounds of incompetence, defect, violation of the law or misappropriation of power and procedure. These are grounds that individuals may invoke to obtain the annulment of an illegal order to shut down a network or services.

Constitutional powers

The Constitutional Court was installed in 2013 but became operational in 2015. It is responsible for monitoring the constitutionality of laws and acts having the force of law. Appeals may also be effected against the unconstitutional use of power by the administrative authorities, making such use of power invalid or unenforceable.

Democratic Republic of Congo

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

No. The Framework Law (see 'Provision of real-time lawful interception assistance' earlier in this chapter for the full statutory citation) is sanctioned with penal provisions and, according to rules and principles of statutory interpretation applicable in the DRC, penal statutes are subject to strict construction. It is not allowed to resolve ambiguities of penal provisions with presumptions: the offence or the exception must clearly be stated in the law; 'decryption' is not stated in the law.

Furthermore, Article 52 of the Framework Law provides that the secrecy of correspondence transmitted through communications is guaranteed by law in the DRC. The confidentiality of correspondence can only be breached strictly in cases of the public interest as provided by the law. Article 53 of the Framework Law reinforces this by stating that the public operator of telecommunications and other telecommunications service providers and members of their staff are required to respect the secrecy of customers' communications.

The legal intercept provisions set forth in clause 55 of the Framework Law do not clearly impose the obligation to decrypt on mobile network operators subjected to lawful intercept obligations. The only actions required under lawful intercept are interception, recording and transcription.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

No. For the reasons set out in Question 1 above.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

A telecommunications operator can offer end-to-end encryption on its communication service without breaching its existing law enforcement obligations. However, a telecommunications operator would need to obtain authorisation (ie, a licence) for the supply of the service from the Regulatory Authority in accordance with the Framework Law. Article 34 of the Framework Law provides that 'cryptology services' means any and all services aimed at transforming, using secret keys, intelligible information or signals into information or signals that are unintelligible for third parties, or vice versa, using hardware or software specifically designed for this purpose. Article 35 of the Framework Law provides that to protect the State's internal and external security and national defence interests, the provision, operation and use of cryptology tools or services are governed by: (1) the prior declaration regime if the tools or service can only be used to authenticate a communication or check the integrity of the message transmitted; and (2) the authorisation regime, with a written consultation of the Ministries responsible for national defence and internal security, in all other cases.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

No such legal precedents exist.

Egypt

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

Constitution of Egypt

Articles 57 and 58 of the Constitution of Egypt explicitly protect the privacy of communications, prohibiting their surveillance except with a reasoned court order for a specific time, in accordance with the law.

The Egyptian Criminal Code and the Criminal Procedures Code

According to the Egyptian Criminal Code (Law 58 of 1937) and the Criminal Procedures Code (Law 150 of 1950), a prosecutor or investigative judge may issue a warrant authorising the interception and recording of individual communications when investigating a possible crime.

Under Article 95 of the Criminal Procedures Code, reasoned warrants from a prosecutor or investigative judge can be issued where they assist in the investigation of any felony or misdemeanour attracting a sentence of over three months, for no more than 30 days and can be renewed once; or by a direct order from an authorised member of the armed forces or security agencies. There are no explicit regulations regarding the latter.

The Communications Law

The Communications Law (Law 10 of 2003) regulates the communications industry, including law enforcement agencies' access to communications and communication infrastructure. It is generally illegal under criminal law to intercept or record private communications except pursuant to a judicial warrant, but the Communications Law allows broad latitude to the armed forces and security agencies to obtain information pursuant to national security concerns, which are not defined.

Article 64 of the Communications Law stipulates that telecom companies must ensure that their communications networks allow the armed forces and the various national security agencies to exercise their authorities under the law.

Article 67 of the Communications Law stipulates that all telecommunications operators and providers shall be subject to the direct administration of competent authorities, and their employees to being summoned, during any circumstances relating to national security. Failure to respond to such summons attracts criminal penalties including imprisonment. National security is defined at the discretion of the authorities.

There is no directly applicable text in the law, but in accordance with Articles 64 and 67 of the Communications Law, the armed forces and national security agencies have broad latitude to intercept communications with or without an operator's control or oversight.

2. Disclosure of communications data

The Egyptian Criminal Procedures Code

The Egyptian Criminal Procedures Code (Law 150 of 1950) gives law enforcement agencies the legal authority to require the disclosure of communications data. Under Article 95 of the Criminal Procedures Code, reasoned warrants from a prosecutor or investigative judge can be issued where they assist in the investigation of any felony or misdemeanour attracting a sentence of over three months, for no more than 30 days and can be renewed once; or the instrument may be a direct order from an authorised member of the armed forces or security agencies. There are no explicit regulations regarding the latter.

3. National security and emergency powers

Except as already outlined above, law enforcement agencies and intelligence agencies do not have any other legal authority to invoke special powers in relation to access to communication service providers' customer data and/or network on the grounds of national security or a state of emergency.

4. Oversight of the use of powers

Applications made pursuant to the Egyptian Criminal Code and the Criminal Procedures Code require a warrant to be issued by a judge. When making an application to the court, the standard is that the court should be satisfied that the warrant is needed for a 'serious effort' to be made investigating the crime in question.

Egypt

Anyone claiming violation of privacy or illegal wiretapping can bring a civil suit for damages or file charges for the use of illegal wiretaps, or seek to have illegally obtained evidence dismissed.

Generally, the armed forces and national security agencies are largely exempt from any control or oversight by the communications regulator, the National Telecommunications Regulatory Authority.

Censorship-related powers

1. Shut-down of network and services

Telecommunications Regulation Law

Article 67 of the Telecommunications Regulation Law (No. 10 of 2003) provides that all telecommunications providers (including Vodafone) are subject to the direct control of the competent government authority, the National Telecommunications Regulatory Authority (the NTRA) in circumstances relating to national security and other major incidents such as natural and environmental disasters or during the declaration of general mobilisation in accordance with the General Mobilisation Law (No. 87 of 1960). In such circumstances, the NTRA, in coordination with the armed forces and the competent authorities, can oblige all telecommunications providers to execute its pre-emptive plan designed for ensuring defence and national security. What constitutes national security is determined by the government. Such control can extend to shutting down a provider's entire network or part of their services.

The NTRA has the power to suspend a telecoms provider's licence if it does not comply with its directions in such circumstances. Telecoms providers have the right to be compensated for damages they suffer as a result of carrying out the plan under Article 68.

2. Blocking of URLs and IP addresses

The Criminal Code

The Criminal Code contains a number of provisions regarding the dissemination of blasphemous or defamatory material, and may be used to legally require any telecoms provider (including Vodafone) to remove such material insofar as possible.

3. Power to take control of Vodafone's network

Telecommunications Regulation Law (No. 10 of 2003)

Please refer to 'Shut-down of network and services' above. It is feasible that this legal power could be used by a competent state authority to take control of a network (such as Vodafone's).

4. Oversight of the use of powers

Telecommunications Regulation Law (No. 10 of 2003)

Under Article 69, employees assigned by NTRA, the armed forces and national security entities may, upon a resolution by the Minister of Justice in coordination with the minister concerned, be considered judicial officers regarding crimes committed in violation of the Telecommunications Regulation Law (No. 10 of 2003) as related to their positions' scope of work. Otherwise there is no judicial oversight of the NTRA's use of its powers.

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes. Articles 57 and 58 of the Constitution of Egypt explicitly protect the privacy of communications, prohibiting their surveillance except [where should this be linking to?] with a reasoned court order for a specific time, in accordance with the law.

According to the Egyptian Criminal Code (Law 58 of 1937) and the Criminal Procedures Code (Law 150 of 1950), a prosecutor or investigative judge may issue a warrant authorising the interception and recording of individual communications when investigating a possible crime.

The Telecommunications Law (Law 10 of 2003) regulates the telecommunications industry, including law enforcement agencies' access to communications and communication infrastructure.

It is generally illegal under criminal law to intercept or record private communications except pursuant to a judicial warrant, but the Telecommunications Law allows broad latitude to the armed forces and security agencies to obtain information pursuant to national security concerns, which are not defined.

Egypt

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

Article 64 of the Telecommunications Law states that:

... All network operators are obliged, at their expense, to allow the armed forces and security agencies access to all their equipment, programs and technical capabilities to enable them to exercise their jurisdiction...

Therefore, the government may seek a telecommunications operator's cooperation in this regard insofar as it is technically possible for the telecommunications operator to assist. However, a telecommunications operator cannot assume the responsibilities or liabilities of a third party, especially those to or over whose network and equipment such an operator has no access or control. In practice, the most that the telecommunications operator could do would be to let the authorities know the contact details for the third party concerned.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

No. According to Article 64 of the Telecommunication Regulation Law, an encryption of telecommunication services by any operator must be approved by the NTRA prior to its application.

The same Article elaborates in the same regard and provides that *All network operators are obliged, at their expense, to allow the armed forces and security agencies access to all their equipment, programs and technical capabilities to enable them to exercise their jurisdiction*, which, according to our interpretation, compels an operator to have the decryption tools – of any encryption solution it may apply – availed for the lawful use thereof by the armed forces and security agencies.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

There are no such examples in this jurisdiction.

France

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time interception assistance

French Criminal Procedure Code

The French Criminal Procedure Code (the CPP) states that, for the investigation of felonies and misdemeanours, if the penalty incurred is at least two years' imprisonment, the investigating judge (*juge d'instruction*) may authorise the implementation of the interception, recording and transcription of telecommunication correspondence where necessary to conduct the investigation. According to Articles 100 and 100-2 of the CPP, the judge's decision must be in writing and issued for maximum period of four months (renewable under the same conditions of form and duration).

Article 706-95 of the CPP states that, as part of investigations relating to organised crime and delinquency, public prosecutors may request from the judge in charge of liberties and custody (the *juge des libertés et de la détention*) an authorisation to implement the interception, recording and transcription of correspondence by telecommunications in accordance with the provisions of Articles 100 ff. of the CPP as mentioned above. The interception may only be ordered for a maximum period of one month, renewable once under the same conditions of form and duration. The judge's decision must be in writing, setting out the justification and granted for a maximum period of four months (renewable under the same conditions of form and duration).

The CPP states that, further to the judge's order, the judge or the police officer appointed by the judge or the public prosecutor may issue a judicial order requiring the telecommunications operator to provide assistance in implementing the interception system.

Under the CPP, interceptions can extend to data stored outside France, as long as access to the data is possible via a terminal in France (Article 57-1, CPP).

For organised crime and terrorism, the CPP permits police, after a judge's approval, to hack into a terminal and create a clone of the computer so as to monitor key strokes from a distance (Article 706-203-1, CPP).

Customs Code

Article 65 of the Customs Code provides that, as part of French customs investigations, the French customs agents may request from telecommunications operators and electronic communication service providers all connection data which the latter retain and process.

French Code of Post and Electronic Communications

Article D98-7-III of the French Code of Post and Electronic Communications (the CPCE) also states that electronic communications networks operators are under an obligation to implement the necessary measures to allow the implementation of interception capabilities as provided for under French legislation.

2. Disclosure of communications data

French Code of Post and Electronic Communications

The CPCE requires, under Article L34-1-III, that electronic communication service providers retain connection data, mainly for the needs of the research, establishment and sanction of criminal offences for a period of up to one year. French law also extends data retention obligations to hosting providers (Article 6-II, law of 21 June 2004). None of these provisions have been modified as a result of the CJEU Digital Rights Ireland case.

Article L32-1-II of the CPCE specifies that electronic communications service providers are required to implement the relevant internal procedures to answer the requests received from public authorities regarding user data. The same applies to access providers.

France

French Criminal Procedure Code

For requests outside the scope of national security, the competent authorities will be required to issue a formal request (*réquisition judiciaire*) to the electronic communications service provider. The competent authority to issue the request will depend on the exact nature of the investigation conducted:

- Requests made in the context of an investigation in 'hot pursuit' (investigations made in 'hot pursuit' are defined by the CPP as investigations conducted when an offence is being committed or has just been committed, as well as when very shortly after the act, the suspect is designated or followed by 'public clamor', or is found with objects or presents traces or clues leading to believe that he or she participated in the offence) can be issued by the public prosecutor in charge of the investigation or by a judicial police officer (Article 60-1 of the CPP).
- Requests made in the context of a preliminary investigation can only be issued by either the public prosecutor in charge of the investigation or by a judicial police officer (Article 77-1-1 of the CPP).
- Requests made in the context of an investigation conducted by an investigation judge may be issued by the judge him- or herself or by a judicial police officer duly appointed by the judge (Article 99-3 of the CPP).

Customs Code

Requests made in the context of an investigation conducted by French customs may be made by an official having at least the rank of 'controller', and do not need the approval of a judge (Article 65 of the Customs Code).

3. National security orders and emergency powers

Code of National Security

France's rules on data gathering for national security purposes were reformed through Law No. 2015-912 of 24 July 2015.

Previously, the legal provisions relating to intelligence gathering were scattered across different provisions of the French Internal Security Code (ISC). Moreover, there has been no single overall supervisory authority for intelligence-gathering activities. The 2015 law rectifies that defect by creating a new independent commission called the Commission for Oversight of Intelligence Gathering Techniques (the CNCTR or 'Commission'). Under the new law, intelligence-gathering measures can be implemented only when a specific authorisation is given by the Prime Minister or his or her designee. The Prime Minister's authorisation is granted only after the Commission has rendered an opinion on the compatibility of the measure with the principles set forth in the law. But the Commission's opinion is not binding on the Prime Minister. Nevertheless, if the Prime Minister decides to ignore the recommendation of the Commission, the Prime Minister must be prepared to explain his or her reasons. Moreover, the Commission can file an appeal with France's Supreme Administrative Court, the Conseil d'Etat, to challenge the Prime Minister's decision.

The law defines intelligence-gathering activity as a measure necessary to protect France's national defence, major foreign policy interests, and major economic, industrial and scientific interests, and to prevent terrorism, immediate threats to public order, organised crime and the proliferation of weapons of mass destruction. Economic espionage is expressly recognised as falling within the remit of the law.

The new law maintains a provision in the Internal Security Code stating that the general monitoring of over-the-air radio transmissions falls outside the code. In other words, untargeted listening of the airwaves by intelligence authorities is permitted without prior authorisation.

Intelligence agencies can obtain access to traffic data from telecoms operators and log data kept by hosting providers, including social media services.

The 2015 law permits intelligence agencies to collect traffic data and log data in real time from telecoms operators and hosting providers, but real-time collection is only possible for the prevention of terrorism. The collection of location data in real time is also permitted.

The most controversial provision in the new law relates to so-called black boxes that intelligence agencies can require operators and hosting providers to install. The law permits intelligence agencies, after authorisation from the Prime Minister, to analyse all traffic and log data on an anonymised basis to identify potential terrorist threats. This analysis is done using algorithms designed to detect suspicious patterns of behavioiur. When it originally presented this provision, the government argued that the data was anonymous and therefore presented no threat to privacy. It is only when suspicious activity is identified that authorities could ask permission to identify the relevant person, and deploy more targeted surveillance. The French data protection authority disagreed, stating that the analysis of metadata involves the processing of personal data and therefore presents a risk for privacy that had to be analysed under strict rules on proportionality.

France

The Constitutional Court did not seem troubled by the black box provision. The Court pointed out that the algorithm only deals with metadata and does not permit the identification of individuals. Moreover, the procedure can only be implemented after an authorisation from the Prime Minister and an opinion from the Commission. The authorisation is only granted for a period of two months and its renewal is subject to certain conditions to ensure that the algorithm does not create too many false positives. Finally, the Court points out that this provision is only allowed in connection with anti-terrorism activities. On balance, the Court felt that the black box provision does not represent a disproportionate restriction on the right to privacy.

Detailed provisions of the ISC:

Article L 871-2 of the ISC states that the competent authorities can request electronic communications network operators provide all necessary information relating to the implementation and exploitation of authorised interceptions.

Article L871-3 of the ISC expressly states that the Ministry in charge of electronic communications must ensure that electronic communication network operators and other electronic communication service providers implement all necessary measures to comply with the obligations imposed as per the provisions of the ISC and of the Code of Criminal Procedure.

The ISC also permits intelligence agencies to require providers of encryption services to provide decryption codes to authorities (Article L 871-1, ISC).

Communications data may be required from the relevant service provider by intelligence agents. The request must in most cases have been authorised by the Prime Minister after a written and justified request sent by the Ministry of Interior, the Ministry of Defence or the Ministry of Economy.

Articles L851-1 and L871-2 of the ISC provide that electronic communications network operators may be asked to provide information and documents processed or retained by their network or electronic communication services, including:

- the technical data relating to the identification of subscription numbers or to the connection to electronic communication services;
- all subscription or connection numbers of a designated individual;
- the location of the terminal equipment used; and
- a subscriber's communications (list of incoming and outgoing calls, length and date of the communications).

Such requests must be made in writing to the CNCTR by the intelligence agents and must be justified.

A dedicated service within the Prime Minister's office is in charge of collecting the information and documents from the operators.

Regarding the prevention of terrorist acts, real-time collection and disclosure of information and documents on operators' networks may be authorised in relation to a specific individual identified as being a threat. The authorisation is granted for a two-month period and renewable under the same conditions.

Operators may also be required, without a court order, to implement automatic processing in order to detect a terrorist threat (Article L851-3 of the ICS), based on parameters defined in the authorisation granted. The automated processing only uses the documents and information referred to by Article L851-1 (see above), only collects the information in accordance with the parameters defined and does not allow user identification. The authorisation is valid for two months and is renewable.

Intelligence agencies have the power to collect metadata (including location data) in real time for terrorism-related investigations (Article L 851-6, ISC).

Electronic correspondence relating to an individual which is likely to reveal information regarding national security, of major interest in foreign politics and the economy, or for the prevention of criminal organised crime, may be intercepted, without a court order. The interception can be extended to the individual's close circle if intelligence agents have reasons to believe the persons close to the individual have valuable information (Article L852-1 of the ISC).

On request of the Ministries of Interior, Defence or Economy, the Prime Minister may authorise, for a renewable one-year period, the surveillance of correspondence or connection data sent or received abroad (Law No. 2015-1556 of 30 November 2015). The prior opinion of the CNCTR is not required for surveillance outside France.

France

4. Oversight of the use of powers

Under Article 100 of the CPP, interceptions are conducted under the authority and supervision of the investigating judge. The same Article expressly states that the decision does not bear the status of a judicial decision and is therefore not subject to appeal before any judge.

Under Article 706-95 of the CPP, interceptions are conducted under the authority and supervision of the judge in charge of liberties and custody. Data subjects are not necessarily informed of the interceptions. Here too, the decision does not bear the status of a judicial decision and is not subject to appeal.

For requests for disclosure of communications data issued in investigations in hot pursuit or in preliminary investigations, the validity of the request may be challenged before the investigations appeal court. The decision itself of issuing a request may not be challenged but its validity (eg if it was not issued by a duly empowered police officer) may be.

For requests issued by an investigation judge, the decision to issue a request may be submitted to appeal by the investigations appeals court.

Requests by the French customs authorities may be challenged before administrative courts.

Interceptions and data collection by intelligence agencies are authorised by the Prime Minister, after a non-binding opinion rendered by the CNCTR. An opinion of the CNCTR is not required, however, if the surveillance measure applies to communications outside French territory. The Prime Minister's orders may be appealed before French administrative courts.

Censorship-related powers

1. Shut-down of network and services

French Code of Post and Electronic Communications

Under Article L36-11 of the French Code of Post and Electronic Communications, the French Regulatory Authority for Postal and Electronic Communications (ARCEP) may, under its own powers or at the request of the Minister responsible for electronic communications, a professional organisation or an approved user association, sanction network operators or electronic communication service providers, for breaching legislative and regulatory provisions relating to their activities. Such sanctions may extend to ordering a full or partial suspension of the operator or service provider's activities. ARCEP's powers could therefore be used to shut down Vodafone's network or certain of its services should Vodafone be found to be in breach of its legislative or regulatory obligations.

A suspension may range from one month to three years, depending on the seriousness of the breach. ARCEP may give the network operator or electronic communications service provider time to resolve the breach before ordering the suspension.

2. Blocking of URLs and IP addresses

Law on Confidence in the Digital Economy of 21 June 2004 as amended on 13 November 2014

The Law on Confidence in the Digital Economy of 21 June 2004 imposes upon network operators (such as Vodafone) the obligation to block without delay access to websites containing content featuring child sex abuse listed by the relevant governmental administrative authority.

Article 6 of the Law also obliges network operators to implement an easily accessible and visible scheme allowing users to report websites containing such content or websites promoting terrorism. They shall inform promptly the competent public authorities of any illegal activities, such as those mentioned above, as well as publicise the means they deploy to fight the said activities.

Law No. 2014-1353 of 13 November 2014 now allows French judicial police to order network operators to block access to content promoting terrorism, through DNS blocking. The police may also order that the content be delisted from search engines. Police already had this power for child pornography. The 13 November 2014 law extends the powers to content promoting terrorism.

Law No. 2015-1501 extending 'state of emergency'

Article 4 of Law No. 2015-1501 adds Article 11 in Law No. 55-385, allowing the Ministry of Interior to block websites promoting terrorism.

Law No. 2010-476 on online gambling

The French online gaming agency (ARJEL) also has the power to seek a blocking order for illegal gambling websites pursuant to Article 61 of Law No. 2010-476 of 12 May 2010 (which is the French law relating to online gambling). In the event that ARJEL identifies an unauthorised gambling website, it will send a cease and desist letter to the online gambling operator. Should the online gambling operator fail to comply with the letter within eight days, the president of ARJEL may request the President of the Paris Tribunal of First Instance to issue a court order for network providers (such as Vodafone) to block access to the offending website.

France

3. Power to take control of Vodafone's network

The French government does not have legal authority to take control of Vodafone's network.

4. Oversight of the use of powers

French Code of Post and Electronic Communications

ARCEP's decisions may be subject to appeal before the highest French administrative court, the Conseil d'Etat.

The Law on Confidence in the Digital Economy of 21 June 2004 as revised by the Law of 13 November 2015

The blocking or delisting of content that promotes terrorism or that contains child pornography is ordered by a special unit of the judicial police, without court supervision. A person designated by the French data protection authority, the CNIL, is informed of each blocking measure and is able to make comments. The CNIL issued its first report on its oversight role on 15 April 2016.

Any person that wishes to challenge a blocking measure ordered by French police may challenge the order before a court. According to the CNIL's report, so far no appeals have been lodged.

Law No. 2010-476 on online gambling

The government's request for a court order requiring network providers to block access to an unauthorised gambling website is reviewed by the court presiding over the request; a court will only make the order if satisfied that it is lawful.

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes. The wording of Article 230-1 of the Criminal Procedure Code (the CPP) has changed slightly (changes underlined here) though the essence is the same:

Where it appears that data seized or obtained during the course of an investigation has been altered, preventing access to or understanding of the information that it contains, the public prosecutor, the investigation court, the police officer authorised by the public prosecutor or the investigation judge, or the court hearing the case, may appoint ***any qualified legal or natural person to carry out the technical operations necessary to obtain a readable version of this information****, and also, where a method of encryption has been used, the secret key for decrypting it, if this appears necessary.*

If the penalty applicable to the offence investigated is of at least two years' imprisonment and the needs of the investigation justify it, the public prosecutor or the examining judge or the relevant court may order the use of 'means protected by official State secrecy'. Subject to restrictions associated with State secrecy, the results of the operations must be provided with technical instructions so that they can be understood and used, as well as a statement provided by the entity which carried out the technical operations certifying the veracity of the results.

Article L871-1 of the Code of National Security (the CNS) states that **legal or natural persons providing encryption services** have to give the decryption keys and decryption methods within 72 hours to competent officers, on the written and specific request of the Prime Minister or of his or her closest authorised member of staff.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

Article 230-1 of the CPP and what follows as well as Article L871-1 of the CNS are broad enough in their scope to include the telecommunications operator ('may appoint any qualified legal or natural person to carry out the technical operations necessary to obtain a readable version of this information').

In addition, a person or entity who is aware of the details of an encryption method which may have been used to prepare, facilitate or commit a crime or a misdemeanour is under an obligation to communicate such information or to assist the authorities upon request according to Article 434-15-2 of the Criminal Code. Failure to do so can give rise to criminal sanctions which may include between three and five years of imprisonment and a criminal fine of between EUR 45,000 and 75,000. This could apply to the telecommunications operator in the present scenario.

France

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

Yes, both on 'business as usual' communication services (where the communication routes over the network as a data packet) and 'over the top' communication services (where the delivery of a communication is made via Internet Protocol (IP) over the network) – as French law does not distinguish (Article L32 of the Postal and Electronic Communications Code). It is possible to offer end-to-end encryption on your communication services without breaching French legislation.

However, in order for a telecommunications operator to be compliant with French law, a number of preliminary formalities may be required, depending on the characteristics of the encryption technology. This would mainly include having to potentially file a declaration with the French Network and Information Security Agency (ANSSI). Indeed, given the heightened level of encryption allowed by end-to-end technology, French authorities (ANSSI for instance) have expressed concerns in relation to such technology, and we understand that they would require a declaration prior to the supply of any end-to-end technology in France.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

Upon initial brief consideration, we are not aware of any specific examples. Given the specific legal provisions available under French law to tackle the sort of situations covered in the area of law enforcement assistance, it is arguably not necessary for the French courts to have to resort to old legislation.

Germany

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

The German Telecommunication Act (*Telekommunikationsgesetz*)

The German Telecommunication Act (**TKG**) requires certain operators of telecommunication systems used to provide telecommunication services to the public to maintain technical and organisational capabilities to execute interception measures provided for by law (Section 110 TKG).

Section 110 TKG requires operators of telecommunication systems used to provide telecommunication services to the public (as further specified in Section 3 TKG) to maintain the technical facilities, and to make the organisational arrangements to execute telecommunication interception measures expressly provided for by law. This includes the obligation to maintain interception capabilities to execute any interception order without delay (including, in particular, handing over a copy of the requested communication). More detailed requirements and specifications, including required technical and organisational standards, are set forth in the Telecommunications Interception Ordinance (*Telekommunikations-Überwachungsverordnung* – TKÜV) and the corresponding Technical Directive issued thereunder (*Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftsersuchen für Verkehrsdaten* – TR-TKÜV).

There are a number of legal statutes that can serve as a legal basis to request the implementation of interception measures, as, for instance, StPO, G10, ZFdG, BKAG and the Police Acts of the federal states as detailed below.

Code of Criminal Procedure (StPO)

The measures pursuant to Section 100a *Strafprozessordnung* (**StPO**) require a prior court order following an application by the public prosecutor's office (or, in relation to tax offences, the tax authority); yet, in pressing circumstances, the public prosecutor's office may also issue an order, which must be confirmed by the court within three working days in order not to become ineffective (Section 100b(1) StPO).

An order may only be granted in cases where certain facts give rise to the suspicion that a serious criminal offence referred to in Section 100a(2) StPO has been committed (or, in cases where there is criminal liability for an attempt, there was an attempt to commit such an offence, or such offence had been prepared by committing a criminal offence), and the offence is one of particular gravity in the individual case as well, and other means of establishing the facts or determining the accused person's whereabouts would be significantly more difficult or even futile (Section 100a(1) StPO).

The measures may only be directed against the accused person or against persons in respect of whom it may be assumed, on the basis of certain facts, that they are receiving or transmitting messages intended for, or stemming from, the accused person, or that the accused person is using their telephone connection (Section 100a(3) StPO).

All persons providing, or contributing to the provision of, telecommunications services on a commercial basis are required to assist the public prosecutor's office (and certain officials working in the police force or, in relation to tax offences, the tax authority) to implement the necessary measures required for the interception/recording of the communication and to provide all necessary information without delay (Section 100b(3) StPO). The measures to be taken are further specified by Section 110 TKG and the TKÜV/TR-TKÜV.

Article 10 Act (Artikel 10-Gesetz-G10)

An order under Section 3 G10 may be granted where actual facts give rise to the suspicion that a serious criminal offence directed against the free democratic basic order or the existence or safety of the Federal Republic of Germany or its federal states (as listed in Section 3(1) G10) will be, is being or has been committed. It may also be granted if a person is part of a group having the purpose of committing such crimes, and the investigation of the facts by other means would be significantly more difficult or even futile.

Measures may be directed against the suspect or a third person who, on the basis of certain facts, is reasonably suspected of receiving or forwarding messages intended for, or stemming from, the suspect (Section 3(2) G10; 'individual interception').

An order under Section 5 (for bundled telecommunications) or Section 8 G10 may be granted where the intercepted information is necessary in order to prevent the danger of an armed attack or terrorist attacks on Germany, international drug trafficking, money laundering or similar crimes that

Germany

will have an impact on German territory (as listed in Section 5(1) G10). It may also be granted to prevent the danger to the life or physical integrity of a person abroad, if such danger directly affects German interests (Section 8 G10).

The interception measures under Section 5 and 8 G10 are not directed at a specific individual. Rather, certain geographic regions are defined as intelligence areas (*Aufklärungsgebiete*), allowing the Federal Intelligence Service to monitor the communication in this area by using certain suitable search terms (Section 5(2) and 8(3) G10; 'strategic interception').

The telecommunication service provider must allow the Intelligence Service to install the relevant technical capabilities on its premises and must grant access to the relevant employees of the Federal Intelligence Service as well as the G10 Commission (Section 110(1) No. 5 TKG and Section 27 TKÜV). The measures to be taken are further specified by the TKÜV/TR-TKÜV.

However, these technical capabilities do not constitute 'interception capabilities' in the direct sense of the term. Rather, the interception itself still has to be performed by the telecommunication provider, which then (electronically) hands over a so-called 'interception copy' (*Überwachungskopie*) of the communication to the Federal Intelligence Service. The communication is filtered by special equipment with the help of pre-defined search terms, and the irrelevant part of the interception copy has to be deleted before the relevant part is passed on to the Federal Intelligence Service.

All persons providing, or contributing to the provision of, telecommunications services on a commercial basis are required to implement the measures to enable the interception/recording of the communication (Section 2(1) G10). The measures to be taken are further specified by Section 110 TKG and the TKÜV/TR-TKÜV.

Customs Investigations Services Act (ZFdG)

Similar rules as under Section 100a and 100b StPO apply under Section 23a and 23b of the ZFdG (which follow the structure and principles of the StPO).

Federal Criminal Police Office Act (BKAG)

Interception orders under Section 20l BKAG are granted via court order upon request by the President of the Federal Criminal Police Office (Section 20l(3) BKAG). Under pressing circumstances, the President of the Federal Criminal Police Office himself can grant the order but has to obtain judicial approval.

Pursuant to Section 20l(1) BKAG, interception orders may be granted in case of imminent danger to the existence or safety of the Federal Republic of Germany, or to the life, physical integrity or freedom of a person, or to objects of substantial value if it lies in the public interest to preserve such objects, or for the purpose of fending off terrorist attacks if there is no other suitable way to prevent such dangers.

All persons providing, or contributing to the provision of, telecommunications services are required to assist the Federal Criminal Police Office to implement the necessary measures required for the interception/ recording of the communication and to provide all necessary information without delay (Section 20l(5) BKAG). The measures to be taken are further specified by Section 110 TKG and the TKÜV/TR-TKÜV.

Police Acts of the federal states

Every German federal state has its own Police Act. These Acts in most cases also set forth similar powers for the state police offices as the BKAG does for the Federal Criminal Police Office, as necessary in order to prevent an imminent danger to the life or physical integrity of a person or in similar precarious situations (see, eg Section 34a, 34b of the Bavarian Police Act, 'BayPAG'). The measures to be taken by the operators of telecommunication systems in assistance of the interception under these state laws are again further specified by Section 110 TKG and the TKÜV/ TR-TKÜV.

In Germany, there appears to be no specific laws that grant government and law enforcement agencies with the legal powers to mandate direct access into a telecommunication service provider's network without the operational control or oversight of the telecommunication service provider.

2. Disclosure of communications data

The German Telecommunication Act (*Telekommunikationsgesetz*)

The German Telecommunications Act (TKG) requires any person providing, or contributing to the provision of, telecommunication services on a commercial basis to provide certain subscriber, line identification and other data upon manual information requests from a range of law enforcement agencies, foreign and domestic intelligence services and other public authorities, where such requests can be based on a legal statutory authorisation (Section 113 TKG).

In addition, Section 112 TKG requires certain providers of publicly available telecommunication services to store certain subscriber, line identification and other data in customer data files to answer automated information requests (handled through the Federal Network Agency *Bundesnetzagentur* – BnetzA) by courts and a range of public authorities.

Germany

Code of Criminal Procedure

The Code of Criminal Procedure, or *Strafprozessordnung* (StPO) further gives the public prosecutor's office (and, in relation to tax offences, the tax authority) the power to acquire certain traffic data relating to customer communications (Section 100g StPO). Similar powers as under Section 100g StPO are granted to the Customs Criminal Investigation Officer under Section 23g ZFdG; to the Federal Criminal Police Office under Section 20m BKAG; to the Federal Office for the Protection of the Constitution under Section 8a BVerfSchG; to the Military Counterintelligence Service under Section 4a MADG; and to the Federal Intelligence Service under Section 2a BNDG.

In addition, certain metadata relating to the circumstances of the communication can be obtained by law enforcement agencies, intelligence agencies and other public authorities entitled under the respective legislative instruments, as part of the interception measures ordered according to Section 100a StPO, Section 20l BKAG, Section 3 G10, Section 23a ZFdG and the respective provisions in the Police Acts of the federal states (see Section 5 and 7 TKÜV). Similar principles apply to measures under Section 5 and 8 G10 (Section 2(1) G10).

Subscriber data, line identification and other data

Section 113 TKG requires any person providing, or contributing to the provision of, telecommunication services on a commercial basis to provide certain subscriber, line identification and other data (specified in Section 95 and 111 TKG) to certain public authorities listed in Section 113(3) TKG (law enforcement agencies, foreign and domestic intelligence services, and other public authorities), as far as necessary for the prosecution of criminal or administrative offences, for averting danger to public safety or order, and/or for the discharge of the legal functions of such agencies.

The request must be made in text form (except in pressing circumstances) and be based on an express legal authorisation. Respective authorisations (which may stipulate further requirements) are, for example, set out in Section 100j StPO, Section 7 and 15 ZFdG, Section 7, 20b and 22 BKAG, Section 22a BPolG, Section 8d BVerfSchG, Section 4b MADG and Section 2b BNDG.

Section 100j StPO gives the public prosecutor's office (and, in relation to tax offences, the tax authority) the power to request, as part of its criminal investigative powers, certain subscriber, line identification and other data, including access control codes (Section 95 and 111 TKG), where the requested information is necessary to establish the facts or determine the whereabouts of the accused person. Where the information request is directed to obtain access control codes, a prior court order following an application by the public prosecutor's office is required; yet, in pressing circumstances, the public prosecutor's office (or certain officials assisting the prosecutor) may also issue an order, which needs to be confirmed by the court without delay. A prior order is not required where the person affected by the request already has or must have knowledge of the request for information or if the use of the data has already been permitted by a court decision.

Similar principles as under Section 100j StPO apply for information requests under the other instruments according to Section 7 and 15 ZFdG, Section 7, 20b and 22 BKAG, Section 22a BPolG, Section 8d BVerfSchG, Section 4b MADG and Section 2b BNDG, as far as the request is necessary for the fulfilment of the respective purposes (eg customs control, the prevention of dangers against the free democratic basic order, terrorist attacks or espionage affairs).

Section 112 TKG requires any provider of publicly available telecommunication services (that in providing commercial telecommunication services allocates telephone numbers or other line identifications or provides telecommunication connections for telephone numbers or other line identifications allocated by others) to store certain subscriber, line identification and other data (specified in Section 111(1) and (2) TKG) in customer data files. These data files must be made available to the BNetzA by means of an automated procedure as necessary for the prosecution of administrative offences under the TKG or the Act Against Unfair Competition (*Gesetz gegen unlauteren Wettbewerb* – UWG) and for answering information requests by certain public authorities (listed in Section 112(2) TKG). Section 112(5) TKG requires the telecommunication services provider to make the technical arrangements in its area of responsibility as required for handling the automated information requests.

The public authorities may only request information from the customer data files, as far as such information is necessary for the discharge of their legal functions (as specified by different legal statutes, such as the StPO, BKAG, ZFdG, BNDG, MADG, BVerfSchG, federal and state Acts on the Protection of the Constitution, and Police Acts on federal and state level). The information request by such public authorities must be made by means of an automated procedure to the Federal Network Agency, which will retrieve and forward such information.

Germany

Traffic data

Section 100g StPO gives the public prosecutor's office (and, in relation to tax offences, the tax authority) the power to obtain traffic data, also without the knowledge of the person concerned.

The measures pursuant to Section 100g StPO require a prior court order following an application by the public prosecutor's office (or, in relation to tax offences, the tax authority); yet, in pressing circumstances, the public prosecutor's office may also issue an order, which must be confirmed by the court within three working days in order not to become ineffective (Section 100g(2) and 100b(1) StPO).

An order may only be granted where certain facts give rise to the suspicion that a person has either committed a criminal offence of substantial significance in the individual case as well (or, in cases where there is criminal liability for an attempt, there was an attempt to commit such an offence, or such offence had been prepared by committing a criminal offence), or has committed a criminal offence by means of telecommunication, and access to the data is necessary to establish the facts or determine the accused person's whereabouts (and further requirements are met).

The measures may be directed only against the accused person or against persons in respect of whom it may be assumed, on the basis of certain facts, that they are receiving or transmitting messages intended for, or transmitted by, the accused person, or that the accused person is using their telephone connection (Section 100g(2) and 100a(3) StPO).

All persons providing, or contributing to the provision of, telecommunications services on a commercial basis are required to assist the public prosecutor's office (as well as certain officials working in the police force or, in relation to tax offences, the tax authority) and to provide all necessary information without delay (Section 100g(2) and 100b(3) StPO).

Similar principles as under Section 100g StPO apply for information requests under:

- Section 23g ZFdG and Section 20m BKAG; and
- Section 8a BVerfSchG, Section 4a MADG and Section 2a BNDG (though only an order by the Ministry of the Interior is required).

In addition, traffic data can be obtained by law enforcement agencies, intelligence agencies and other public authorities entitled under the respective legislative instruments, as part of the interception measures ordered according to Section 100a StPO, Section 20l BKAG, Section 3 G10, Section 23a ZFdG and the respective provisions in the Police Acts of the federal states (see Section 5 and 7 TKÜV). Similar principles apply to measures under Section 5 and 8 G10 (Section 2(1) G10). The StPO gives courts and public prosecutors (and certain officials assisting the prosecutor's office and, in relation to tax offences, the tax authority) the power to request, as part of their criminal investigative powers, the disclosure and, as necessary, the seizure of stored customer communications (Section 94 et. seqq. 98 StPO). This applies to emails on the provider's mail server and likely also applies to voicemails and similar communications stored by the provider.

Where the content of customer communications is yet to be considered part of an ongoing telecommunication process, then the content of the communication may only be accessed by means of an interception order according to Section 100a and 100b StPO. This also comprises communications that are placed in or retrieved from a storage facility, which is assigned to the primary identification that is to be intercepted (Section 5(1) No. 3 TKÜV).

The request for disclosure under Section 94 and 95 StPO does not require a prior judicial order. Where the request is not complied with, the public prosecutor's office (or, in relation to tax offences, the tax authority) may initiate the formal seizure of the stored communication according to Section 94 ff., 98 StPO.

The seizure of stored communications requires a prior court order; yet, in exigent circumstances, the public prosecutor's office (or certain officials assisting the prosecutor's office) may also issue an order. An official who has seized the communication without a prior court order must apply for a court confirmation within three days if neither the person concerned nor a relative was present at the time of seizing the information (or such persons have declared their objection). The person concerned by the seizure may request a court decision at any time (Section 98 StPO).

The order may be granted where there is sufficient probability of a suspicion of a criminal offence and the stored communication may be of importance as evidence for the criminal investigation (subject to a strict proportionality test and a balancing of all the interests involved).

3. National security and emergency powers

Except as already outlined above, the German government does not have the legal authority to invoke special powers in relation to access to a communication service provider's customer data and/or network on the grounds of national security.

German government agencies do not have special powers that can be invoked in time of national crisis or emergency.

Germany

4. Oversight of the use of powers

Code of Criminal Procedure (StPO)

As well as what is set out above, according to Section 101 StPO, the participants in the telecommunication under surveillance must be notified of any interception measures, including their option to obtain subsequent court relief, unless there are overriding conflicting interests of an affected person. Notification must take place as soon as it can be effected without endangering the purpose of the investigation or the life, the physical integrity and/or personal liberty of a person, or significant assets. For up to two weeks following their notification, the participants may apply to the competent court for a review of the lawfulness of the measure, as well as of the manner and means of its implementation. The participants may file a complaint against the court's decision.

There is a dispute if and to what extent the operator of a telecommunication system is entitled to file a complaint (according to Section 98(2) or 304(2) StPO) against an interception order issued under Section 100a StPO, though it is recognised that there is no legal obligation to verify or challenge the lawfulness of an interception order.

Article 10 Act

There is no ex-ante judicial control for measures under the Article 10 Act, ie no court order or warrant is required. However, the interception measures pursuant to Section 3, 5 and 8 G10 require a written order by the Ministry of the Interior (or the relevant highest state authority) following an application by one of the public authorities authorised under the respective provision.

In addition, the so-called G10 Commission may at any time examine – following a complaint or also of its own volition – the admissibility and necessity of the ordered measures.

There are no legal remedies available for a person concerned by an interception measure under Section 3 G10 as long as such measure is not yet communicated to the person (Section 13 G10). After this communication, the person concerned can challenge the interception order before the administrative courts. A communication to the concerned person shall be made after the measure has been completed, unless such communication may endanger the purpose of the interception measure or may cause overall harm for the wellbeing of the federation or its states.

Customs Investigations Services Act (ZFdG)

For measures under the ZFdG, similar principles as for measures under Section 100a and 100b StPO apply (see, in particular, Section 23c ZFdG).

Federal Criminal Police Office Act (BKAG)

The measures pursuant to Section 20l BKAG require a prior court order following an application by the President of the Federal Criminal Police Office; yet, in pressing circumstances, the President of the Federal Criminal Police Office may also issue an order, which must be confirmed by the court within three working days in order not to become ineffective (Section 20l(3) BKAG).

According to Section 20w BKAG, the participants in the communication under surveillance must be notified of any interception measures, including their option to obtain subsequent court relief, unless there are overriding conflicting interests of an affected person. Notification must take place as soon as it can be effected without endangering the purpose of the investigation or the life, the physical integrity and/or personal liberty of a person, or significant assets. The participants may file a complaint against the court's decision.

Police Acts of the federal states

Similar rules as under the BKAG apply under the Police Acts of the federal states (though details may differ from state to state).

Subscriber data, line identification and other data

For manual information requests under Section 113 TKG, the judicial oversight and legal remedies depend on the specific different legal statutes granting the authorisations for the information requests.

For information requests pursuant to Section 100j StPO, no prior court order is required, except where the information request is directed to obtain access control codes (following an application by the public prosecutor's office or, in relation to tax offences, the tax authority); in exigent circumstances, the public prosecutor's office (or certain officials assisting the prosecutor or, in relation to tax offences, the tax authority) may also issue such an order, which then needs to be confirmed by the court without delay. A prior order is not required where the person affected by the request already has or must have knowledge of the request for information or if the use of the data has already been permitted by a court decision.

Germany

The person concerned must be notified of the information request only in certain cases (relating to data enabling access to terminal devices and requests based on the use of IP-addresses), and only if there are no overriding conflicting interests of an affected person (Section 100j(4) StPO). The notification must take place as soon as it can be effected without endangering the purpose of the information request. The person concerned may challenge the lawfulness of the measure in front of the courts.

Similar rules as under Section 100j StPO apply for information requests under Section 20b BKAG (which follows the same structure and principles).

For information requests under Section 8d BVerfSchG, Section 4b MADG and Section 2b BNDG, no prior court order is required. However, where the information request is directed to obtain access control codes, a prior order by the Ministry of the Interior is necessary (following an application by the respective responsible authority).

For automated information requests under Section 112 TKG, the judicial oversight and legal remedies depend on the specific different legal statutes defining the legal functions and powers of the public authorities.

Traffic data

In addition to the above, according to Section 101 StPO, the participants in the telecommunication concerned by the measure surveillance must be notified of any disclosure of their traffic data, including their option to obtain subsequent court relief, unless there are overriding conflicting interests of an affected person. Notification must take place as soon as it can be effected without endangering the purpose of the investigation or the life, the physical integrity and/or personal liberty of a person, or significant assets. For up to two weeks following their notification, the participants may apply to the competent court for a review of the lawfulness of the measure, as well as of the manner and means of its implementation. The participants may file a complaint against the court's decision.

There is a dispute if and to what extent the telecommunication service provider is entitled to file a complaint (according to Section 98(2) or 304(2) StPO), though it is recognised that there is no legal obligation to verify or challenge the lawfulness of a request.

Similar principles as under Section 100g StPO apply for information requests under Section 23g ZFdG and Section 20m BKAG.

For information requests under Section 8a BVerfSchG, Section 4a MADG and Section 2a BNDG, no prior court order is required.

However, a prior order by the Ministry of the Interior is necessary (following an application by the respective responsible authority).

With regard to information requests that are ancillary to interception measures according to Section 100a StPO, Section 20l BKAG, Section 3, 5 and 8 G10, and Section 23a ZFdG, the respective judicial oversight procedures for these interception measures extend to the information requests.

The request for disclosure does not require a prior judicial order but may be challenged by the person concerned before the courts.

The seizure of stored communications requires a prior court order; yet, in pressing circumstances, the public prosecutor's office (or certain officials assisting the prosecutor's office or, in relation to tax offences, the tax authority) may also issue an order.

An official who has seized the communication without a prior court order must apply for a court confirmation within three days if neither the person concerned nor a relative was present at the time of seizing the information (or such persons have declared their objection). The person concerned by the seizure may request a court decision at any time.

A seizure order by a court may be challenged by the person concerned by filing a complaint.

Censorship-related powers

1. Shut-down of network and services

German Telecommunications Act

Section 126 of the German Telecommunications Act entitles the Federal Network Agency (the Bundesnetzagentur) to order 'necessary measures' if a network provider violates its obligations under the Act or the EU Roaming Regulation. These measures can extend to the whole network service, or parts of it; however, the measures must be proportionate and only as intrusive as required by the circumstances. Therefore, the Federal Network Agency has the power to order Vodafone to shut down some or all of its network or services, if it determines this to be a necessary measure.

There is a three-step procedure for measures under Section 126: first, the network provider is given a deadline (usually one month) to remedy its violation; if it fails to do so within the deadline, the Federal Network Agency can order measures necessary to remedy the violation. In certain cases, the Federal Network Agency can deviate from this procedure and order necessary preliminary measures at the outset; this is usually when

Germany

the network provider's violation endangers public safety and order or causes substantial disadvantage to other network providers or users. In case of a severe or repeated violation, the Federal Network Agency may ultimately prohibit a network provider from providing its network or services.

The Federal Network Agency also has powers under Section 115 if a network provider does not fulfil its obligations with regard to public security (for example, data security or technical safety measures). The procedure under Section 115 is similar to the procedure outlined above, with the exception that no preliminary measures can be ordered.

2. Blocking of URLs and IP addresses

Interstate Broadcasting Treaty

Section 59(3) of the Interstate Broadcasting Treaty (the *Rundfunkstaatsvertrag*) entitles the State Media Authorities (the *Landesmedienanstalten*) to order necessary measures if a website breaks the law. These measures can extend to requesting a network provider (such as Vodafone) to block access to the website, although this is a last resort and should only be called upon if other measures have failed to remedy the problem. In practice, the State Media Authorities usually receive references from the police or public prosecutor's office with respect to websites that breach the law before taking any of the aforementioned measures.

3. Power to take control of Vodafone's network

The government does not have the legal authority to take control of Vodafone's network.

4. Oversight of the use of powers

German Telecommunications Act

In case of preliminary measures under Section 126 of the German Telecommunications Act, the concerned party is heard by the Federal Network Agency. The Federal Network Agency then decides whether to maintain, alter or set aside its order.

Additionally, because Sections 115 and 125 provide for administrative acts, they can be challenged before Germany's administrative courts.

Interstate Broadcasting Treaty

All measures under Section 59(3) of the Interstate Broadcasting Treaty constitute administrative acts and therefore can be challenged before Germany's administrative courts.

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes. According to Section 8(3) of the Telecommunications Interception Ordinance (TKÜV), which applies to interception measures under the German Code of Criminal Procedure (StPO), the Article 10 Act (G10), the Customs Investigations Services Act (ZFdG), the Federal Criminal Police Office Act (BKAG) and the Police Acts of the federal states, an operator of a telecommunication system (a Telco Communication Service Provider, CSP) has to remove all encryption measures it has applied to the communication data before delivering an interception copy of the communication to the authorities.

As stated above, this obligation only applies to operators of telecommunication systems (Telco CSPs). However, according to Section 100b (3) of the German Code of Criminal Procedure (StPO), every telecommunication service provider (ie also an Over the Top (OTT) CSP) has to comply with judicial orders requiring them to provide data and information on the communication which might also include providing the respective data in a readable (ie decrypted) format.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

There is no express statutory obligation in this regard in Germany. Section 8(3) of the Telecommunications Interception Ordinance (TKÜV) only applies to encryption mechanisms that have been applied by the operator (Telco CSP) itself and not by third parties and thus according to its wording does not entail an obligation to (try to) remove third-party encryption mechanisms.

The compliance obligations of telecommunication service providers (Telco CSPs as well as OTT CSPs) under Section 100b (3) of the German Code of Criminal Procedure (StPO) can naturally only relate to measures that are in their capacity and within the range of reasonable measures. Thus, we are of the view that the government generally does not have the authority to expressly require the telecommunications operator to (try to) decrypt data from third-party OTT services on this basis.

Germany

In case an 'equipment interference' by the telecommunications operator is possible, however, this could be construed to fall within the scope of compliance obligations of telecommunication service providers (Telco CSPs as well as OTT CSPs), pursuant to Section 100b (3) of the German Code of Criminal Procedure (StPO), and the government might be able to request this from Vodafone. However, according to our research, there are no precedents in this regard in Germany, and it is doubtful whether a court would deem such a measure adequate and reasonable (note: we have not reviewed whether such interference is admissible from a criminal law point of view).

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

Generally, there is no statutory provision in Germany prohibiting providers from offering end-to-end encryption. However, there is an ongoing discussion whether further legal regulations should be introduced in this regard in view of the technical progress and the difficulties the government is facing when trying to access encrypted data but, so far, no legislative action has been taken.

However, the interpretation of the German statutory law is somewhat complex in this area.

As for BAU services, the statutory law could be interpreted in a way as to suggest that a Telco CSP may not offer end-to-end encryption. This depends on how it is to be interpreted that Section 8(3) of the Telecommunications Interception Ordinance (TKÜV) only applies to encryption mechanisms that have been applied by the provider itself and not by third parties. Technically, the end-to-end encryption is applied by the customer and not by the telecommunications operator. As a result, it could be stated that the telecommunications operator cannot be obliged to remove the encryption under this provision as it has not applied the encryption itself.

On the other hand, as the telecommunications operator itself offers the software making the end-to-end encryption possible and only the factual encryption is applied by the customer, it could also be said that it is an encryption applied by the telecommunications operator and therefore would have to be removed by the telecommunications operator in case of an interception order. As a consequence, if a telecommunications operator cannot remove an encryption in accordance with national law enforcement obligations, it is not allowed to apply it.

The interpretation of the law in this regard likely also depends on whether the customer is able to decide on a case-by-case basis whether the encryption is applied.

All in all, we are of the view that it is likely that this does not prevent Telco CSPs from offering end-to-end encryption to their customers. There are several voices in legal literature that agree with this view and the fact that there is an ongoing discussion on how law enforcement authorities could be enabled to better access encrypted communication shows that it is generally considered to be the 'problem' of the government whether they are able to obtain decrypted information and, on the other hand, that telecommunication service providers are not prohibited from offering or applying such encryption in the first place.

As Section 8(3) of the Telecommunications Interception Ordinance (TKÜV) only applies to Telco CSPs, OTT CSPs would not be affected by the above and would be allowed to offer end-to-end encryption to their customers.

Law enforcement authorities may also implement technical measures on their own in order to be able to intercept encrypted communication data before it is encrypted by secretly installing certain software applications on the user's equipment. This is called a 'lawful interception at the source' (*Quellen*-TKÜ). Although it is sometimes seen critical that the telecommunications provider is in no way involved in this interception, it is still considered to be legitimate and is regularly performed by the government. However, such interception at the source – like almost all interception measures by the government – can only be implemented if approved and ordered by a judge and if a severe crime is investigated.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

To our knowledge, there are no such examples in Germany.

Ghana

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

The Electronic Communications Act 2008 (Act 775) (the ECA)

Under Section 100 of the ECA, the President may, by executive instrument, make written requests and issue orders to operators or providers of electronic communications networks or services requiring them to intercept communications and provide any user information or otherwise in aid of law enforcement or national security.

The Anti-Terrorism Act 2008

According to the Anti-Terrorism Act, 2008 (Act 762) a senior police officer (not below the rank of an Assistant Commissioner of Police) with the written consent of the Attorney-General and Minister of Justice (AG) may apply to a court for an order to require Vodafone to intercept customer communications for the purpose of obtaining evidence of commission of an offence under the Anti-Terrorism Act.

2. Disclosure of communications data

The Electronic Communications Act 2008 (Act 775) (the ECA)

The ECA gives the power to the National Communication Authority (NCA) and certain public authorities to obtain metadata relating to customer communications such as traffic data, service use information and subscriber information.

Under Section 4(2)(a) of the ECA, telecommunications providers have an obligation to provide information required by the NCA for regulatory and statistical purposes. Section 8(2) authorises the NCA to request the disclosure of lists of subscribers, including directory access databases. Section 68 of the ECA empowers the NCA to request information from service providers concerning the communications network, the use of spectrum granted and the use of the communications network or service.

Regulation 103 of the Electronic Communications Regulations 2011 (LI 1991)

Regulation 103 of the Electronic Communications Regulations, 2011 (LI 1991) also requires telecommunications providers to submit to the verification of electronic communications traffic by the NCA.

The Electronic Transactions Act 2008 (Act 772) (the ETA)

Under Section 101 of the ETA, the government or a law enforcement agency may apply to a court for an order for the disclosure of customers' communications that are in transit or held in electronic storage in an electronic communications system by a communications service provider.

3. National security and emergency powers

The Electronic Communications Act 2008 (Act 775) (the ECA)

Under the ECA, during a state of emergency, communications service providers are required to give priority to requests and orders for the transmission of voice or data that the President considers necessary in the interests of national security and defence.

Section 99 of the ECA states that where a state of emergency is declared under the Constitution or any other law, Vodafone will be required to give priority to requests and orders for the transmission of voice or data that the President considers necessary in the interests of national security and defence.

Section 99(6) gives power to the President to assume direct control of electronic communications services and issue operation regulations in the event of a declaration of war.

4. Oversight of the use of powers

Regarding applications made pursuant to the Anti-Terrorism Act 2008, a senior police officer will first require the written consent of the Attorney-General before making an application to court and seeking judicial approval.

Applications made under section 101 of the Electronic Transactions Act, 2008 (Act 772) by the government or a law enforcement agency must first go to the court to seek judicial approval. Then, an order can be granted relating to the disclosure of customers' communications that are in transit or held in electronic storage in an electronic communications system by a communications service provider. The court will not make the order unless it is satisfied that the disclosure is relevant and necessary for investigative purposes or is in the interests of national security.

There is no judicial oversight or approval of the use of powers under the Electronic Communications Act 2008 (Act 775) (the ECA).

Ghana

Censorship-related powers

1. Shut-down of network and services

The Electronic Communications Act 2008 (Act 775) (the ECA)

Under Section 99(6) of the Electronic Communications Act 2008 (Act 775), the President may assume direct control of communications services in times of war. The powers are wide and likely to include the power to order a shut-down of networks and/or services.

2. Blocking of URLs and IP addresses

See Section 1 'Shut-down of network and services' above; given the wide nature of the President's powers, it is likely that he or she would be able to order the blocking of URLs and IP addresses.

3. Power to take control of Vodafone's network

See Section 1 'Shut-down of network and services' above.

4. Oversight of the use of powers

There is no judicial oversight of the President's powers under Section 99(6) of the Electronic Communications Act 2008 (Act 775).

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes. Under Section 99(3) of the Electronic Transactions Act 2008, a law enforcement officer with a court warrant may require the telecommunications operator to provide access – and to decrypt information if necessary – to customer data in connection with the investigation of an offence.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

Under the Electronic Transactions Act 2008, a law enforcement officer with a court warrant may require a telecommunications operator to provide access to decryption information, code or technology necessary to decrypt customer data in connection with the investigation of an offence. Such decryption information, code or technology could include 'equipment interference' technology.

A telecommunications operator may be required to provide such information, code or technology even where the encryption is applied by a third party to the extent that the telecommunications operator has access to the decryption information, code or technology. It is questionable whether the telecommunications operator could be legally compelled to decrypt encryption that has been applied by a third party given that, practically, this would usually mean that the telecommunications operator would not have access to the decryption information, code or technology. We are not aware of any legal precedent in this area. There is no reported case law on the subject matter.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

Currently, there is no law expressly prohibiting a telecommunications operator from doing so. The National Communications Regulations 2003 (LI1719) encourage operators to employ international best practices in the telecommunication industry to promote privacy, secrecy and security of communications carried or transmitted by them, or through their communications system, and of the personal and account data related to their subscribers. Thus, if the purpose of the end-to-end encryption is to encourage confidentiality of its subscribers, a telecommunications operator can proceed to implement the service with prior written notice to the National Communications Authority.

We note, however, that the Electronic Transactions Act 2008 (Act 772) mandates the National Information Technology Agency to establish a Certifying Agency whose functions include issuing licences and monitoring the conduct of an encryption service provider. The Certifying Agency is yet to be established. Until the Certifying Agency is established, the National Information Technology Agency (NITA) is required to act in the interim. NITA is, however, yet to commence the licensing or regulation of encryption services in Ghana. When NITA or the Certifying Agency (when established) commence the implementation of the relevant provisions of the Electronic Transactions Act, the telecommunications

Ghana

operator may be required to obtain a licence from NITA or the Certifying Agency in order to carry out its end-to-end encryption on the BAU Service. OTT service providers providing end-to-end encryption services may also be required to register with NITA or the Certifying Agency except when they are licensed by foreign licensing authorities recognised by NITA or the Certifying Agency.

That said, there is no legal precedent that we are aware of which addresses whether the introduction of end-to-end encryption, which would disable a telecommunications operator's ability to comply with its existing law enforcement assistance obligations under the Electronic Communications Act 2008 and Anti-Terrorism Act 2008, would put a telecommunications operator in breach of those laws. There is no reported case law on the subject matter.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

The laws on encryption and lawful interception in Ghana are relatively new and undeveloped. We are not aware of any such precedent.

Greece

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

According to Article 19(1) of the Greek Constitution, the confidentiality of communications is absolutely inviolable; however, there are conditions under which a judicial authority is not bound by such confidentiality, where national security or particularly serious crimes are involved.

Law 2225/1994 was adopted on the basis of Article 19(1) of the Greek Constitution and sets out the procedure that judicial or other public authorities should follow when requesting the withdrawal of confidentiality. An application for the withdrawal of confidentiality (which would allow for the interception of individual customer communications) can only be made for reasons of national security (Article 3) or for the purposes of identifying certain criminal offences (Article 4). Withdrawal of confidentiality is also permitted in order to investigate the crimes listed in Article 253A and 253B of the Hellenic Criminal Procedure Code.

For the withdrawal of confidentiality, an order is issued by the competent judicial authority on the basis of Article 5 of Law 2225/1994. The order includes information on the public authority, public prosecutor or investigator requesting the withdrawal, the purpose of the withdrawal, the means of communication which form the object of the withdrawal and, in the case of criminal offences being investigated, the name of the person against whom the withdrawal is directed as well as his or her residential address. The excerpt of the order, containing its operative part, is delivered to the Chairman, Board of Directors, General Manager or representative of the company concerned (Article 5(4) of Law 2225/1994).

According to Article 6(1) of Presidential Decree 47/2005 (issued in order to provide the procedure for the withdrawal of confidentiality as this is stipulated by Law 2225/1994), when a competent authority seeks the execution of an order, a service provider, having the technical equipment and software available, is obliged to activate the equipment and software required for the withdrawal of confidentiality within three hours from notification of the order, regardless of the time when the order was actually served and, in cases of urgency, which have to be specifically mentioned, as early as possible. Article 7(2) of Presidential Decree 47/2005 specifies that the execution of an order for the withdrawal of confidentiality is performed by the competent authority in cooperation with the service provider.

In addition, the Hellenic Authority for Communications Security and Privacy (ADAE) was formed as a result of Article 1 of Law 3115/2003 and has issued guidelines on the measures that service providers, such as Vodafone, should have in place in order to ensure that confidentiality is protected during the real-time interception of communications (ADAE Decisions 52/2009 and 53/2009).

Following the execution of an order, one or more reports are prepared by the service that was involved in the withdrawal of confidentiality and these are submitted to the judicial authority that issued the order as well as to ADAE and the applicant authority (Article 5(5) of Law 2225/1994). Confidentiality cannot be withdrawn for a period of time that exceeds two months unless extensions are granted by the competent judicial authorities. However, extensions of the initial time of two months cannot exceed the time limit of two months per case and, in total, may not exceed a period of 10 months. Such restriction does not apply in cases where the withdrawal of confidentiality is ordered for reasons of national security (Article 5(6) of Law 2225/1994). The judicial authority that ordered the withdrawal of confidentiality may order its removal even before the expiry of the time set, if the purpose of the measure has been fulfilled or the reasons for its implementation no longer exist (Article 5(8) of Law 2225/1994).

2. Disclosure of communications data

Article 4 of Presidential Decree 47/2005 lists the specific communications data that a service provider may be required to disclose and this includes the content of customer communications and metadata, depending on the type of communication involved.

Law 3917/2011 (Article 1.1) states that the providers of publicly available electronic communications services or of public communications networks are obliged to retain certain data which are produced or processed by them, so that this data may be made available to the competent authorities for the identification of particularly serious criminal offences, as these are defined

Greece

in Article 4 of Law 2225/1994. The law applies to traffic and location data on both legal entities and natural persons, and to the related data necessary to identify the subscriber or registered user. It does not apply to the content of electronic communications. According to Article 8(1) of Law 3917/2011, disclosure of communication data is performed according to the provisions of Law 2225/1994.

3. National security and emergency powers

In the event of war, mobilisation due to external threats or an immediate threat to national security, or an armed coup to overturn democracy, under Article 48 of the Greek Constitution, the Greek Parliament has the power, following the government's recommendation, to implement special measures. It is possible that such measures could include direct access to a service provider's network to enable interception, although this is not expressly mentioned. The validity of these measures is limited to a period of 15 days; however, this term may be extended fortnightly by separate decisions of the Greek Parliament.

The decision of the Greek Parliament to adopt special measures in this situation is taken in one sitting by a three-fifths majority of the total number of members. In deciding to extend their duration, a majority of members must vote in favour in one sitting.

4. Oversight of the use of powers

Following the execution of an order, one or more reports are prepared by the service that was involved in the withdrawal of confidentiality and these are submitted to the judicial authority that issued the order, as well as to ADAE and the applicant authority (see Article 5(5) of Law 2225/1994).

Confidentiality cannot be withdrawn for a period of time that exceeds two months, unless extensions are granted by the competent judicial authorities. However, such extensions may not exceed, in total, a period of 10 months. Such restriction does not apply in cases where the withdrawal of confidentiality is ordered for reasons of national security. The judicial authority that ordered the withdrawal of confidentiality may order its removal even before expiry of the time set if the purpose of the measure has been fulfilled or the reasons for its implementation no longer exist.

Censorship-related powers

1. Shut-down of network and services

Law 4070/2012

Although the power to shut down a network is not expressly provided for, Article 3(a) of Law 4070/2012 states that restrictions may be imposed on the operation of a network for the purposes of safeguarding public order, security and health.

Under Article 20(9)(c) the Minister of Infrastructure, Transport and Networks, upon the recommendation of the Hellenic Telecommunications & Post Commission (EETT), can prohibit the provision of any electronic communications service within a specific radio spectrum range, provided this is sufficiently justified by the need to ensure safety of life. Exceptionally, the Minister may extend these measures to fulfil other objectives in the public interest.

EETT has the authority to revoke or suspend a service provider's operating licence in Greece (known as a 'General Licence') where serious or repeating breaches of the telecoms law have been committed, pursuant to Article 77 of Law 4070/2012.

Regulation on the Use and Assignment of Rights for the Use of Radio Spectrum

Article 14(2) of EETT's Regulation on the Use and Assignment of Rights for the Use of Radio Spectrum states that an entity's right to use radio spectrum may be suspended where this is in the public interest.

2. Blocking of URLs and IP addresses

Constitution of Greece

Article 5A(1) of the Greek Constitution states that all persons have the right to information (and to participate in the internet 'information society'), as such constitutional provision is specified by the relevant legislative provisions. Restrictions may be imposed by law only as far as they are absolutely necessary and justified for reasons of national security, combating crime or protecting the rights and interests of third parties. Facilitation of access to electronically transmitted information, as well as of the production, exchange and diffusion of it, constitute an obligation of the State, in compliance with Articles 9, 9A and 19 of the Constitution of Greece.

Greece

Presidential Decree 131/2003

Under Article 2(4) of Presidential Decree 131/2003 the State has the power to adopt restrictive measures with respect to information society services originating from other EU member states if these measures are necessary for reasons relating to public order (especially the protection of minors and the fight against incitement to hatred because of religion, nationality, etc), protection of public health, public security, national security and defence, as well as the protection of consumers and investors.

Presidential Decree 109/2010

Article 4 of Presidential Decree 109/2010 states that the Greek National Council for Radio and Television may prohibit the retransmission, by any means, of television programmes originating from other EU member states which manifestly, seriously and gravely infringe the rules concerning the protection of minors and/or incite hatred on grounds of race, sex, religion or nationality, disability, age and sexual orientation.

Similarly, the Greek National Council for Radio and Television can take measures to restrict or prohibit the provision, by any technical means, of on-demand audio-visual media services from other EU member states, including for breach of the rules previously mentioned.

Law 4002/2011, Article 48(10) and Article 51(5)

In the gaming sector, pursuant to Law 4002/2011, internet service providers are prohibited from providing access, attempted by an IP address located in Greece, to websites of gaming operators who have not obtained a Greek licence, the details of which are included in a black list that is kept by the Hellenic Gaming Commission.

3. Power to take control of Vodafone's network

Constitution of Greece

Under Article 48 of the Constitution of Greece, in the event of war, mobilisation due to external threats, an immediate threat to national security or an armed coup to overturn democracy, the Parliament has the power, following the government's recommendation, to implement special measures. In this case, applicability of Article 19 of the Constitution of Greece, among others, may be suspended. Potentially, such measures could include taking control of Vodafone's network, although this is not expressly mentioned. The validity of these measures is limited to a period of 15 days, although this term may be extended fortnightly by Parliament.

The decision of the Parliament to adopt special measures in a national emergency situation must be taken in one sitting by a three-fifths majority of the total number of its members. In deciding whether to extend the duration of those special measures, a majority of members of the Parliament must vote in favour of the extension in one sitting.

4. Oversight of the use of powers

Decisions taken by public authorities, such as EETT, are subject to judicial review by the competent administrative courts.

The measures adopted pursuant to Article 20(9)(c) of Law 4070/2012 are reviewed regularly and at least every two years, at which point the results of the review are published.

Greece

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes. Article 8(7) of Presidential Decree 47/2005 expressly provides that, during the execution of an order, a service provider who encrypts data should deliver or forward the requested data in decrypted form. According to Article 8(9) of Presidential Decree 47/2005, service and network providers are obliged to provide competent authorities with:

a. all interfaces from which requested communication data may be transferred to monitoring facilities;
b. communication content and data at the time communication is carried out;
c. information and assistance in order to be verified that communication data reaching the interface are identical to the target; and
d. assurances that the reliability of the interconnection system is at the same level as the one offered through provided services to subscribers and users.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

No explicit reference is made in statutory law to encryption applied by a third party; however, the following may apply:

Article 3(1) of Presidential Decree 47/2005 expressly states that the withdrawal of confidentiality refers to any type of communication which is being carried out either through a communications network or through a service provider and by a subscriber or user against whom the withdrawal of confidentiality is being ordered.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

There are no specific statutory rules applicable to end-to-end encryption in this type of scenario. However, as it results from the spirit of the law, service and network providers should always be in a position to cooperate with the authorities and provide the requested information.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

There are no such legal precedents in Greece.

Hungary

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

National Security Services Act

Act CXXV of 1995 on the National Security Services (the **National Security Services Act**); Act XXXIV of 1994 on the police (the **Act on Police**); and Act XIX of 1998 on Criminal Proceedings (the **Criminal Proceedings Act**) give the competent court and in the case of the intelligence agencies under the National Security Services Act, the Minister of Justice, the power to authorise the interception of a person's communications following an application made by the relevant intelligence agency or law enforcement agency (LEA).

Electronic Communications Act

Under Section 92(1) of Act C of 2003 on Electronic Communications (the **Electronic Communications Act**), electronic communications service providers in Hungary are required to cooperate with organisations authorised to conduct covert investigations and to use their facilities in their electronic communications systems so as not to prevent or block covert investigations, eg interceptions.

In addition, under Section 92(2) of the Electronic Communications Act, at the written request of the National Security Services, electronic communications service providers are required to conclude an operational agreement with the National Security Services within 60 days concerning the application of the means and methods of covert investigation operations.

Criminal Proceedings Act

Under Section 202(6) of the Criminal Proceedings Act, interception by LEAs may only be conducted if obtaining evidence by other means appears unlikely to succeed or would involve unreasonable difficulties, and there is probable cause to believe that evidence can be obtained by the interception.

Under Section 71 of the Act on Police and Section 203 of the Criminal Proceedings Act, the competent court can issue an order for interception. Under Sections 57–58 of the National Security Services Act, the competent court or the Minister of Justice can issue an order for interception.

Government Decree on Cooperation

The Electronic Communications Act and Government Decree No. 180/2004 on the rules of cooperation between electronic communications service providers and authorities authorised for secret data collection (the **Government Decree on Cooperation**) requires electronic communications service providers to cooperate with LEAs and intelligence agencies in relation to covert investigations and the set-up and maintenance of interception equipment.

Under Section 3(a) of the Government Decree on Cooperation, electronic communications service providers must ensure, among other things, that all conditions necessary for the implementation of tools in relation to covert investigation operations are provided; for example, a lock-up where the necessary equipment can be placed and the provision of non-stop technical assistance, if required.

Under Sections 3(3) and 6(3) of the Government Decree on Cooperation, LEAs and intelligence agencies can implement technical devices so that they have direct access to the networks of electronic communications service providers, without the personal assistance of the employees of the service providers.

2. Disclosure of communications data

Electronic Communications Act

Under Section 157(10) of the Electronic Communications Act, intelligence agencies, courts and a range of other public authorities have the power to acquire the metadata relating to customer communications, including, among others, traffic data, the IMEI number, service use information and subscriber information, but not the content of the communications.

Under Section 92(2) of the Electronic Communications Act, electronic communications service providers may be required to disclose the content of stored customer communications (eg voicemail), if available. Electronic communications service providers cannot be required to store the content of customer communications.

Act on the Police

Under Section 68 of the Act on the Police, if a request is made by the police in relation to serious crimes (as set out under Section 68 of the Act on the Police), the supply of data cannot be refused.

National Security Services Act

Under Section 11(5) of the National Security Services Act, the competent minister investigates complaints made in relation to the activities of the intelligence agencies.

Hungary

In addition, lawful process and transfer of personal data is also monitored by the National Authority for Data Protection and Freedom of Information, the president of whom hears and investigates complaints about any alleged misuse of personal data.

3. National security and emergency powers

Except as already outlined in this report, government agencies do not have any other legal authority to invoke special powers in relation to access to communication service providers' customer data and/or networks on the grounds of national security.

Electronic Communications Act

Under Section 37(1) of the Electronic Communications Act, for the protection of human lives, health and physical integrity, or for the protection of the environment, public safety and public policy, or for the prevention of dangers exposing significant threats to a broad range of users, or that directly jeopardise the operations of other service providers and users, a resolution may be adopted on the prohibition of the provision of any service or the use of radio frequencies.

Under Section 37(1) of the Electronic Communications Act, the National Media and Infocommunications Authority (the Authority) may pass a resolution on the prohibition of the provision of any service or the use of radio frequencies.

4. Oversight of the use of powers

No appeal can be submitted against the relevant resolution of the Authority in relation to the prohibition of the provision of any service or the use of radio frequencies. However, judicial review of the resolution can be requested from the competent court.

Interception is subject to the prior, or in urgent cases the subsequent, approval of the court/minister. No appeal can be submitted against an order of the court/minister unless the interception resolution is in relation to an ongoing investigation under the Criminal Proceedings Act.

Censorship-related powers

1. Shut-down of network and services

Electronic Communications Act

Under Section 37(1) of the Electronic Communications Act, the National Media and Communications Authority (the NRA) may pass a resolution prohibiting the provision of any particular network or telecommunications service or the use of specified radio frequencies. Such a resolution may be made for the protection of human life or health; for the protection of the environment; the protection of public safety and public policy; or to prevent situations where there is an imminent and direct threat jeopardising the operation of network operators or other businesses. Such a resolution would have the effect of requiring Vodafone to shut down its network or services.

Act on State of Emergency

Under Section 64(2)–(4) of the Act on State of Emergency, a resolution requiring the temporary limitation or shut-down of electronic communications may be ordered. Such resolution may be made by the Committee of National Security, the President of Hungary or the Hungarian government, depending on the specific type of state emergency. Under Sections 48–52 of the Fundamental Act of Hungary, generally a 'state of emergency' is declared where there is war, threat of war, or internal armed conflicts. In a state of emergency, the shut-down of Vodafone's network or services may be ordered.

2. Blocking of URLs and IP addresses

Media Services Act CLXXXV of 2010

Section189(4) of the Media Services Act CLXXXV of 2010 gives the power to Hungary's Media Council to order electronic communications service providers, such as Vodafone, to temporarily block certain online content by blocking the relevant IP addresses.

Act on Gambling

Under Section 36/G of the Act on Gambling, the National Tax and Customs authority may order the blocking of sites on which illegal gambling is made available.

Hungary

3. Power to take control of Vodafone's network

Act on State Emergency

Under Section 64(2)–(4) of the Act on State Emergency, a resolution ordering the takeover of control of electronic communications devices may be adopted by the Committee of National Security, the President of Hungary or the Hungarian government, depending on the specific type of extraordinary circumstance. While 'electronic communications device' is not defined, it is considered likely that in such circumstances, the government, president or committee would be inclined to adopt a broad interpretation. Therefore, it is feasible that these powers could be used to take control of a network provider's network (such as Vodafone's).

4. Oversight of the use of powers

Electronic Communications Act

A resolution of the NRA prohibiting the provision of any particular network or telecommunications service or prohibiting the use of specified radio frequencies cannot be appealed. However, judicial review of the resolution can be requested from the competent court.

Act on State Emergency

The rules for legal remedies at the time of a state emergency are not presently specified; they are determined at the time of the emergency.

Criminal Procedures Act

Powers to order the blocking of IP addresses under Section 158/B(2) of the Criminal Procedures Act and Section 77 of Act C of 2012 of the Criminal Code are exercised by the criminal court.

Act CLXXXV of 2010

A resolution of the Media Council to temporarily block IP addresses is subject to judicial review if a request for judicial review is made to the competent court.

Act on Gambling

The operator of the blocked site may request the review of the blocking resolution at the court.

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes. Under Section 6 (2) of the Government Decree on Cooperation and Section 71 (1) of the Criminal Procedures Act, electronic communications service providers must restate, decrypt or expand any altered, encrypted or compressed information.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

Section 71(1) of the Criminal Procedures Act explicitly regulates that if a court, public prosecutor or investigation authority contacts an electronic communications service provider to provide data, the contacted service provider is obliged to make the content of encrypted data available, if possible. If decryption is technically not possible, the telecommunications operator is obliged to notify the requesting authority about the inability of performance within the set timeframe.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

Under Section 3(4) of the Government Decree on Cooperation, electronic communications service providers may not carry out any development of their systems or services that excludes or makes covert investigation impossible.

Under Section 92(1) of Act C of 2003 on Electronic Communications (the Electronic Communications Act), electronic communications service providers must carry out their activities in such a way that it does not exclude or make covert investigation impossible.

Under Section 92 (3) of the Electronic Communications Act, electronic communications service providers are obliged to inform the National Security Services about any activity, service or product or any change thereof, which affects or influences the proper operation of covert investigations.

Hungary

In addition, under Section 92(4) of the Electronic Communications Act and Section 3(2) of the Government Decree on Cooperation, electronic communications service providers are required to ensure the application conditions of means and methods necessary for the recognition of transmitted messages forwarded through its network in the scope of covert investigation.

On the basis of the above, electronic communications service providers may not offer end-to-end encryption on its communication services regardless of being a BAU or an OTT service provider.

A new law on counterterrorism amended Act CVIII of 2001 on Electronic Commerce and on Information Society Services and introduced the definition of application service provider. An application service provider is defined as 'a natural person or legal entity who or which provides access to a software or hardware through electronic communication network, provides software application or any related services through a specific software or web surface to multiple users, limited or unlimited in time, for monthly or use-based consideration or for free'.

According to this law, if an application service provider offers encrypted services (other than end-to-end encryption), it will be required to retain the content of the conversation, together with any data originated or managed in relation to such content, for one year, and shall deliver it to the authority carrying out any covert investigation, if so requested.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

We are not aware of any relevant historical cases regarding encryption. We note, however, that in Hungary there is no precedent law, meaning that judicial decisions cannot be based only on similar historical cases.

India

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Background

Indian Telegraph Act 1885 (ITA)

This is the parent legislation governing telecommunications in India and the government grants the following licences to service providers in accordance with the provisions of this Act:

Unified Access Service Licence (UASL)

This is the licence governing access services in India.

Internet Service Provider (ISP) Licence

This is the licence governing internet access services in India.

Unified Licence (UL)

The Department of Telecommunications in 2013 issued the Unified Licence which is an umbrella licence encompassing all services such as access, internet, national long distance and international long distance. This implies that a service provider can provide all services under a single licence. Current UASL and ISP licensees will have to migrate to the Unified Licence Regime on expiry of their existing licences. For the purposes of this report, we have relied on the UASL and ISP licences, highlighting differences in the UL where applicable.

Information Technology Laws

The laws generally governing communications over the internet are as follows:

a. **Information Technology Act 2000 (IT Act)** This is the parent legislation governing information technology in India. It empowers the government to undertake various forms of electronic surveillance and censorship in accordance with procedures prescribed in the IT Rules 2009.

b. **IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 (Interception Rules)** These Rules specify the procedure the government must follow to intercept, monitor and decrypt electronic information stored, generated, transmitted or received in any computer resource.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

Under Section 5(2) of the ITA read with Rule 419-A (I) of the Indian Telegraph Rules 1951 (ITR), during a public emergency or in the interests of public safety, either the Secretary to the Ministry of Home Affairs (in the case of the central government) or the Secretary to the Home Department (in the case of the state government) or a person above the rank of Joint Secretary (in unavoidable circumstances) authorised by the respective government may issue a written order directing an interception, if the official in question believes that it is necessary to do so in:

a. the interests of sovereignty and integrity of India;

b. the security of the state;

c. friendly relations with foreign states;

d. public order; or

e. the prevention of incitement of offences.

In the case of an emergency, the prior approval of the government officials referred to above may be dispensed with. In such a case, the interception or monitoring will have to be carried out by an officer not below the level of the Inspector General of Police.

Section 69 of the IT Act permits authorised government officials to intercept or monitor information transmitted, generated, received or stored in any computer. Accordingly, the service provider is required to extend all technical facilities, equipment and technical assistance to the authorised government officials to intercept the information and to provide information stored in the computer. The Interception Rules lay down the procedure to be followed by the government to authorise such interception or monitoring.

Under Section 69 of the IT Act read with Rule 3 of the Interception Rules, either the Secretary to the Ministry of Home Affairs (in the case of the central government) or the Secretary to the Home Department (in the case of the state government) or a person above the rank of Joint Secretary authorised by the respective government (in unavoidable circumstances) may issue an order for the interception of any electronic information transmitted, stored or generated over any computer if the official in question believes that it is necessary to do so in:

a. the interests of sovereignty and integrity of India;

b. the security of the state;

c. friendly relations with foreign states;

d. public order; or

e. the prevention of incitement of offences.

India

The UASL and the ISP Licence require the licensee to implement the necessary facilities and equipment for interception purposes in terms of the following provisions:

1. Clause 41.20(xvi) of the UASL and Clause 34. 28(xvi) of the ISP Licence require the licensee to provide the necessary hardware/software in their equipment to enable the government to enable interception and monitoring from a centralised location.
2. Under Clause 34.4 and Clause 41.7 of the ISP Licence, the licensee is required to install the equipment that may be prescribed by the government for monitoring purposes.
3. Under Clause 34.28(xiv) of the ISP Licence and Clause 41.20(xiv) of the UASL, in the case of remote access of information, the licensee is required to install suitable technical devices enabling the creation of a mirror image of the remote access information for monitoring purposes.
4. Clause 41.10 of the UASL Licence requires the licensee to install the necessary hardware/software to enable the government to monitor simultaneous calls.

Under Rule 13 read with Rule 19 of the Interception Rules, once the interception order has been issued according to Rule 3 of the Interception Rules, an officer not below the rank of the Additional Superintendent of Police will make a written request to the intermediary to provide all facilities and the necessary equipment for the interception of the information.

Section 2(w) of the IT Act defines intermediary to include 'telecom service providers, network service providers and internet service providers'.

Licences

The UASL is entered into between a telecom service provider and the Department of Telecommunication (DoT) for the provision of telecommunications services. The ISP Licence is entered into between an internet service provider and the DoT for the provision of internet services. Under both the UASL and the ISP Licence, licensees are bound to take all steps and provide all facilities to enable the government to intercept communications. Clause 42.2 of the UASL and Clause 35.5 of the ISP Licence require the licensee to provide the necessary interception facilities required under Section 5 of the ITA.

Clause 41.10 of the UASL and Clause 34.6 of the ISP Licence provide designated government officials with the right to monitor telecommunications traffic at any technically feasible point. The licensee is required to make arrangements for simultaneous monitoring by the government.

Clause 34.8 of the ISP Licence requires each ISP to maintain a log of all connected users and the service that they are using. The ISP is also required to maintain every outward login. The logs and the copies of all the packets originating from the Customer Premises Equipment (CPE) of the ISP must be made available in real time to the government.

2. Disclosure of communications data

Legislation

The Code of Criminal Procedure (CrPC) empowers a court or police officer in charge of a police station to seek the production of 'any document or other thing' if the officer believes that the document is necessary for the purposes of any investigation.

Section 69 of the IT Act permits authorised government officials to intercept or monitor information transmitted, generated, received or stored in any computer. Accordingly, the service provider is required to extend all technical facilities, equipment and technical assistance to the authorised government officials to intercept the information and to provide information stored in the computer.

Licences

Under the UASL and the ISP Licence Agreement, the licensee is required to provide access to all call data records as well as any other electronic communication. Under Clause 41.10 of the UASL, the licensee is required to provide the call data records of all the calls handled by the licensee as and when required by the government.

With respect to the ISP Licence Agreement, Clause 33.4 requires the licensee to provide the government with the required tracing facilities to trace messages or communications, when such information is required for the investigation of a crime or for national security purposes.

Section 91 of the CrPC permits a court or officer in charge of a police station to issue either a summons or written order requiring the production of 'any document or other thing necessary or desirable for the purposes of any investigation, inquiry, trial or proceeding'.

Section 69 of the IT Act permits authorised government officials to 'intercept or monitor information transmitted, generated, received or stored in any computer'. Accordingly, the service provider is required to extend all technical facilities, equipment and technical assistance to the authorised government officials to intercept the information and to provide information stored in the computer.

Interception has been defined under Rule 2(l) of the Interception Rules to include the acquisition of 'the contents of any information' through any means in so far as it enables the content of the information to be made available to a person other than the intended recipient.

India

3. National security and emergency powers

Legislation

Under Section 5(1) of the ITA, if there is a public emergency or in the interests of public safety when the government believes it is necessary, the government has the power to temporarily take possession of the 'telegraph' established and maintained, or worked on, by any person authorised under the ITA.

Licences

The government has the following special powers under the UASL and the ISP Licence:

1. Under Clause 41.13 of UASL and Clause 10.5 of the ISP Licence, the government may 'take over the service, equipment and networks of the licensee' in the event that such directions are issued in the public interest by the government in the event of a national emergency, war, low-intensity conflict or any other eventuality.
2. Under Clause 41.1 of UASL and Clause 34.1 of the ISP Licence, the licensee must 'provide necessary facilities depending upon the specific situation at the relevant time to the Government to counteract espionage, subversive act, sabotage or any other unlawful activity'.
3. Under Clause 41.5 of UASL and Clause 5.1 of the ISP Licence, the government may revise the licence clauses at any time if 'considered necessary in the interest of national security and public interest'.
4. In terms of Clause 41.11 of UASL and Clause 34.9 of the ISP Licence, the government may, through appropriate notification, block the usage of mobile terminals in certain areas of the country. In such cases, the licensee must deny service in the specified areas within six hours of receiving the request.
5. Under Clause 41.20(xviii) of UASL and Clause 34.28(xviii), the government may restrict the licensee from operating in any sensitive area on national security grounds.

In addition, Clause 33.7 of the ISP Licence and Clause 39.14 of the UL provide that the 'use of the network for anti-national activities' (such as breaking into an Indian network) may be deemed sufficient reason to revoke the licence, and will be considered an offence punishable under criminal law.

The ITA, the UASL and the ISP Licence do not prescribe the method and the instrument that the government may use in this regard.

4. Oversight of the use of powers

There is no judicial oversight over the interception process.

With respect to the review of the interception of telephonic communication under the ITA and the ITR, a Review Committee has been established under Rule 419-A(16) of the ITR at both central and state level. According to the ITR, every order issued by the relevant government officials has to be sent to the Review Committee.

The Review Committee is required to meet once every two months and if the Review Committee is of the opinion that an interception order was not in accordance with the provisions of the ITA and the ITR, it may set aside the interception order and also order the destruction of the information obtained through interception.

Under Rule 419- A(17), if the interception has been carried out in an emergency, the relevant government official has to be informed of such interception within three working days and the interception has to be confirmed within seven working days. Otherwise, the interception will have to cease and the same message cannot be intercepted without the prior approval of the Union or state Home Secretary.

A similar Review Committee has also been established under the Interception Rules. Rule 22 of the Interception Rules provides for the establishment of a Review Committee to examine the interception or monitoring directions. If the Review Committee is of the opinion that the interception or monitoring directions are not in accordance with Section 69 of the IT Act, then it may set aside the direction and also order the destruction of the information obtained through interception.

Censorship-related powers

1. Shut-down of network and services

Indian Telegraph Act 1885

On the occurrence of a public emergency or in the interests of public safety, the government, if it believes it is necessary, may temporarily take possession of a provider's network (such as Vodafone's network) pursuant to provisions of the Indian Telegraph Act 1885. This power, however, is subject to the licence conditions stated below, and the fundamental rights of the citizens envisioned under the constitution of India.

India Department of Telecommunication – UAS Licence and ISP Licence

India's Department of Telecommunication licenses telecommunications service providers under its Unified Access Service Licence Agreement (UAS Licence) or Unified Licence Agreement (UL Licence), and internet service providers under its Internet Service Provider Licence Agreement (ISP Licence).

Under the terms of these licences, the government may, in the public interest, issue directions entitling it to take over the service, equipment and networks of the licensee in the event of a national emergency, war, low-intensity conflict, or any other eventuality.

India

Additionally, under the licence terms, the government through appropriate notification, may debar usage of mobile terminals, and require the licensee to deny services, as may be prescribed, in certain areas of the country. The licensee must deny service in the specified areas within six hours of receipt of the request. Therefore, Vodafone may be required to cease providing services in certain areas, if required by the government.

This should be read in light of any and all Addenda and Amendments to the licence conditions, as may be made from time to time.

2. Blocking of URLs and IP addresses

Information Technology Act 2000

Under Sub-section (1) of Section 69A of the Information Technology Act 2000, the central government, or any of its officers specially authorised by it in this behalf (acting through an officer not below the rank of Joint Secretary), has the power to direct telecommunications providers, network providers and internet service providers to block public access to any information generated, transmitted, received or stored in any computer resource. The officer giving the direction may only do so, if he or she believes it is necessary, in the interests of protecting the sovereignty and integrity of India, defending the security of the state, protecting public order, maintaining friendly relations with foreign states or preventing incitement to the commission of any recognisable offence relating to the above. Therefore, Vodafone may sometimes be required by the government to block public access to information accessed on its network. In practice, this is likely to be by blocking a URL or IP address.

The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009 (known as the 'Blocking Rules'), stipulate the procedure to be followed in such matters. Under the Blocking Rules, the designated officer may, on receipt of any request from the nodal officer of an organisation, or from a competent court, by order, direct any agency of the government or intermediary to block access by the public to any information or part thereof, generated, transmitted, received, stored or hosted in any computer resource, for any of the reasons specified under Sub-section (1) of Section 69A of the Information Technology Act. Upon receipt, the government reviews the request according to the detailed procedure set forth in the Blocking Rules, and, if it believes it necessary, may issue a written order (acting through the designated officer), requiring access to the website to be blocked.

India Department of Telecommunication – Licences

In addition to the above, the government has the authority under the ISP Licence to direct all ISP licensees, like Vodafone, to block websites and/or individual subscribers, in the interests of national security or public interest.

Information Technology (Intermediaries Guidelines) Rules 2011

Under Rule 3 of the Information Technology (Intermediaries Guidelines) Rules 2011, a telecoms provider, network provider or internet service provider is required to take down content once it knows that the content is in violation of Rule 3. The content must be taken down within 36 hours. Usually the type of content to which this rule applies is content which contains information that is grossly harmful, harassing, blasphemous, defamatory or otherwise illegal or offensive.

3. Power to take control of Vodafone's network

See the powers outlined in 'Shut-down of network and services' above.

4. Oversight of the use of powers

The aforementioned prohibitory orders can be issued only by persons with appropriate authority, after following due process. Such orders, if any, must be passed judiciously by the appropriate governmental or regulatory authorities, within the framework of applicable legal provisions, licence conditions, and the constitutional rights of the citizens; otherwise, the orders would be subject to judicial scrutiny.

An order may be challenged on legitimate grounds before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) , or in a court with appropriate jurisdiction over the matter.

India

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes. Section 69 of the IT Act (see 'Provision of real-time lawful interception assistance' above) empowers designated government officials to direct any agency to decrypt, intercept or monitor or to cause the decryption, interception or monitoring of any information transmitted, generated, received or stored in any computer resource. This provision may be used to compel decryption by intermediaries including Telco CSPs, OTT CSPs and OTT services.

Subsequent to a direction being issued, intermediaries or subscribers who are in charge of the target computer resource are required to extend all facilities and technical assistance as may be required by the agency implementing the direction.

The Interception Rules lay down the procedure required to be followed by the government to authorise such decryption under Section 69 of the IT Act. The Interception Rules state that either the Secretary to the Ministry of Home Affairs (in the case of the central government) or the Secretary to the Home Department (in the case of the state government) or, in unavoidable circumstances, a person not below the rank of Joint Secretary to the Government of India duly authorised, may issue a direction for the decryption of any information transmitted, stored or generated over any computer resource.

In the case of an emergency where obtaining prior approval of the competent authorities is not feasible, decryption may be carried out with the prior approval of the Head or second most senior officer of the concerned agency at central level, or of an officer not below the rank of Inspector General of Policy at state level.

Furthermore, Clause 37.1 of the Unified Licence (UL) (which is defined at the beginning of this chapter) places a general prohibition on the use of bulk encryption by licensees, and empowers the government or designated officers to evaluate any encryption equipment connected to the licensee's network. Clauses 23.2 and 39.12 of the UL require the licensee to procure and provide, at its own cost, monitoring and interception equipment and facilities which may be required by the licensor. Clause 39.1 also requires the licensee to provide necessary facilities to the government to counter espionage, subversive acts, sabotage or any other unlawful activity.

Additionally, the UL makes it clear that the use of encryption by subscribers will be subject to the policy laid out in the IT Act and rules made thereunder. In this regard, it may be noted that while no policy has been finalised, the government (in October 2015) issued, and subsequently withdrew, a draft of the National Encryption Policy. This draft policy was widely criticised for its onerous plaintext retention requirements and its proposal to impose caps on key lengths and algorithms that may be deployed.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

As discussed in Question 1, the power to issue decryption directions emanates from Section 69 of the IT Act and the IMD Rules.

Under the IMD Rules, a 'decryption direction' means a direction issued to a decryption key holder to disclose a decryption key or provide decryption assistance (Rule 2(h)). In this regard, the Rules define a 'decryption key holder' to mean any person who deploys the decryption mechanism and who is in possession of a decryption key for decryption of encrypted communications (Rule 2(j)). Moreover, Rule 13 of the IMD Rules states that any decryption direction issued to an intermediary will be limited to the extent the information is encrypted by the intermediary or that the intermediary has control over the decryption key.

Therefore, unless a telecommunications operator is in possession of the decryption key concerned, the government is unlikely to be able to require the telecommunications operator to decrypt or interfere with encrypted communications where encryption is carried out by third parties. However, this would not preclude the government from seeking the telecommunications operator's assistance in acquiring/intercepting the encryption key where possible.

As discussed in Question 1, under the UL, any licensee is required to provide all possible assistance and facilities in relation to interception, monitoring and decryption as may be required by the government, depending on the specific situation at hand. However, it is likely that for the purpose of issuing decryption directions and orders, the substantive provisions and procedure contained within the IT Act framework would prevail.

India

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

See the response to Question 1 above for background information relating to the general decryption framework applicable under Indian law.

As discussed above, a licensee to the UL is required to provide all possible assistance and facilities in relation to interception, monitoring and decryption as may be required by the government depending on the specific situation at hand. Additionally, licensees are required under various clauses of the UL (including Clauses 32 and 40) to ensure compliance with all provisions of the Indian Telegraph Act 1885 – including Section 5 of the Act empowering the government to intercept messages.

As end-to-end encryption would frustrate the provisions of Section 5 of the ITA and lead to the telecommunications operator being unable to comply with its provisions, the telecommunications operator is likely to be prohibited under the terms of the UL from deploying the same.

Note that, in addition, the government is empowered under the IT Act to issue a policy relating to modes and methods of encryption that may be used. In this regard, while no policy has been finalised, the government (in October 2015) issued and subsequently withdrew, a draft of the National Encryption Policy. This draft policy was widely criticised for its onerous plaintext retention requirements and its proposal to impose caps on key lengths that may be deployed. The legality of end-to-end encryption would therefore be subject to the final policy set out by the government.

In early May 2016 a petition was filed in the Supreme Court of India alleging that the deployment of end-to-end encryption by OTT services (such as WhatsApp and Telegram) violates provisions of Indian law including provisions of the IT Act, Telegraph Act and IMD Rules. The petition is currently in its preliminary stages of hearing.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

To our knowledge, there are no such examples available in the public domain.

Ireland

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

The Postal and Telecommunications Services Act 1983 as amended by the Postal Packets and Telecommunications Messages (Regulation) Act 1993

The Postal and Telecommunications Services Act 1983 (the **1983 Act**) (as amended by the Postal Packets and Telecommunications Messages (Regulation) Act 1993 (the **1993 Act**)) establishes a regime for the interception of telecommunications messages under Irish law. Although 'telecommunications message' is not defined for these purposes, it is likely to include emails and SMS messages as well as phone calls, etc.

Section 110 of the 1983 Act provides that the Minister for Posts and Telegraphs (now the Minister for Communications, Energy and Natural Resources) (the Minister) may issue directions in writing to a Licensed Operator requiring them to do (or refrain from doing) anything which the Minister may specify from time to time as necessary in the national interest. As a direction by the Minister is a specific exception to the prohibition on interception of telecommunications messages under Section 98 of the same Act, it is clear that the Minister may issue a direction in writing to mobile network operators requiring them to intercept individual customer communications. As such, it would seem that the Minister's powers are sufficiently broad to require Licensed Operators to assist in implementing interception capabilities on their networks. However, for such a direction to authorise the implementation of interception capabilities on a Licensed Operator's network (such as Vodafone's network), the direction would need to very specifically refer to this. Furthermore, under Section 110 of the 1983 Act, the Minister's powers seem sufficiently broad to allow implementation of a technical capacity that enables direct access to a Licensed Operator's network (without the Licensed Operator's operational control or oversight).

In addition, Section 2 of the 1993 Act states that the Minister for Justice may give an authorisation of interception in writing or in a case of exceptional urgency, orally, for the purpose of criminal investigation or in the interests of the security of the State. The definition of 'interception' contained in Section 1 in the 1993 Act would seem to encompass the interception of individual customer communications. The Minister for Justice is specifically empowered to enable another person to intercept a telecommunications message, and as such, the powers of the Minister for Justice would seem sufficiently broad to require Licensed Operators to assist in implementing interception capabilities on their networks. However, for such an authorisation to require the implementation of interception capabilities on, for example, Vodafone's network, the authorisation would need to specifically refer to this.

Applications for an authorisation of interception under Section 2 of the 1993 Act must be made in writing by the Garda Commissioner or the Chief of Staff of the Defence Forces for the purpose of criminal investigation or in the interests of the security of the State.

Section 2(5) of the 1993 Act provides that authorisations of interception under Section 2 of the 1983 Act shall remain in force for a maximum of three months, unless extended for a further three months at a time under Section 2(6) of the 1993 Act.

Postal and Telecommunications Services (Amendment) Act 1999

Section 7 of the Postal and Telecommunications Services (Amendment) Act 1999 (the **1999 Act**) applies the provisions of the 1983 Act and the 1993 Act relating to directions, authorisations and warrants for the interception of telecommunications messages to telecommunications operators licensed under the 1983 Act (Licensed Operators). As Vodafone is a Licensed Operator, it is subject to the interception regime set out in the 1983, 1993 and 1999 Acts and as such, may be required to intercept individual customer communications.

Criminal Justice (Surveillance Act) 2009

Section 4 of the Criminal Justice (Surveillance) Act 2009 (the **2009 Act**) states that a superior officer of the Garda Síochána (the Irish police), the Defence Forces or the Revenue Commissioners may apply to a judge for an authorisation to carry out surveillance where they have reasonable grounds for believing that it is necessary for a criminal investigation into, or the prevention of the commission of, an arrestable offence (Garda Síochána and Revenue Commissioners) or maintaining the security of the State (Garda Síochána and Defence Forces).

Ireland

Section 1 of the 2009 Act defines 'surveillance' as:

i. monitoring, observing, listening to or making a recording of the movements, activities and communications of a particular person/group of persons; or

ii. monitoring or making a recording of places or things by or with the assistance of surveillance devices.

As such, the powers granted to Irish law enforcement agencies under Section 4 of the 2009 Act seem sufficiently broad to allow the implementation of a technical capability that enables direct access to a Licensed Operator's network (without the Licensed Operator's operational control or oversight).

Applications for authorisations of surveillance under Section 4 of the 2009 Act can be made to any District Court judge on sworn evidence by a member of the Garda Síochána, not below the rank of chief superintendent, or an officer of the Permanent Defence Force, not below the rank of colonel, in order to safeguard the security of the State where to do so is justified.

In addition, a member of the Garda Síochána or a member of the Defence Forces may carry out surveillance without an authorisation under Section 7 of the 2009 Act if the surveillance has been approved by a superior officer in circumstances where the security of the State would otherwise be likely to be compromised.

2. Disclosure of communications data

Communications (Retention of Data) Act 2011

Section 6 of the Communications (Retention of Data) Act 2011 (the **2011 Act**) allows for the making of requests to service providers to disclose customer data retained in accordance with Section 3 of the 2011 Act (a **Disclosure Request**).

Section 1 of the 2011 Act defines 'service provider' as a 'person engaged in the provision of a publicly available electronic communications service or a public communications network by means of a fixed line or mobile telephone or the Internet' (referred to herein as a **Licensed Operator**). As Vodafone falls within the definition of a service provider, it is subject to the retention and disclosure of data regime set out in the 2011 Act.

In addition, Schedule 2 of the 2011 Act details the types of information in relation to fixed network and mobile telephony which must be retained by Licensed Operators, for two years:

i. the names and addresses of subscribers or registered users; and

ii. the data necessary to identify the location of mobile communication equipment.

The types of information in relation to internet access, internet email and internet telephony which must be retained by Licensed Operators for one year:

i. the names and addresses of subscribers; and

ii. registered users to whom IP addresses, user ID or telephone numbers are allocated.

Disclosure Requests under Section 6 of the 2011 Act can be made by a member of the Garda Síochána, not below the rank of chief superintendent, an officer of the Permanent Defence Force, not below the rank of colonel, or an officer of the Revenue Commissioners, not below the rank of principal officer. Such parties may request a Licensed Operator to disclose customer data retained in accordance with Section 3 of the 2011 Act where the data is required for:

i. the prevention, detection, investigation or prosecution of a serious offence (Garda Síochána and Revenue Commissioners);

ii. the safeguarding of the security of the State (Garda Síochána and Defence Forces); and

iii. the saving of human life (Garda Síochána and Defence Forces).

Under Section 6(4) of the 2011 Act, Disclosure Requests should be made in writing, or in a case of exceptional urgency, orally.

Law enforcement agencies in Ireland may obtain search warrants under a wide array of legislation. Such search warrants may be issued in respect of stored customer data, which may require Vodafone to provide copies of relevant metadata relating to customer communications and to disclose the content of stored customer communications, including voicemails.

Law enforcement agencies in Ireland may also obtain Orders requiring persons to show a member of the Garda Síochána any material which is in their possession which is likely to be of substantial value in the context of certain criminal investigations or proceedings (**Disclosure Orders**), under a variety of statutes including the Central Bank (Supervision and Enforcement) Act 2013, the Criminal Justice Act 2011 and the Taxes Consolidation Act 1997. Such Disclosure Orders may require Vodafone to provide copies of relevant metadata relating to customer communications and to disclose the content of stored customer communications.

The extent of the powers of an Irish law enforcement agency under a search warrant will depend on the particular statutory provisions under which the warrant has been issued. There is no standard regime in relation to search warrants in Irish law, and warrants may be issued under approximately 200 different statutes. It is therefore difficult to outline the exact obligations which all such warrants impose.

The powers under a warrant will generally include, as a minimum, a power to enter premises, to search the premises for relevant evidence, and to seize and retain anything which may be regarded as evidence. Further

Ireland

powers, such as the power to put certain questions to persons present on the premises, and to require the assistance of such persons, are also common.

While warrants are generally issued to the Garda Síochána, they may also be issued to other law enforcement bodies including the Competition Authority, the Office of the Director of Corporate Enforcement and the Revenue Commissioners, in connection with offences over which they have jurisdiction.

Disclosure Orders are similar to search warrants, and may include a power to enter premises and to search for the relevant material. However, the focus of Disclosure Orders is on obtaining material from third parties, and they operate in the first instance as a direction to the third party to produce the relevant material, rather than a power for law enforcement agencies to enter premises and seize it. Disclosure Orders often include a provision stating that where the relevant information is not in legible form, the subject of the Order shall be required to give the password to the information to enable the law enforcement agency official to examine the information or produce the information in a form in which it is, or can be made, legible and comprehensible. The exact extent of the powers of an Irish law enforcement agency under a Disclosure Order will depend on the particular statutory provisions under which the Disclosure Order has been issued. For example, the provisions dealing with Disclosure Orders in some Acts, such as the Criminal Justice Act 1994, specifically refer to information held on computers. There is no standard regime in relation to Orders to make material available in Irish law, and such Orders may be issued under a number of different statutes.

3. National security and emergency powers

Except as already outlined above, the government does not have any other legal authority to invoke special powers in relation to access to Licensed Operators' customer data and/or network on the grounds of national security.

There do not seem to be any additional special powers bestowed on the government in times of emergency.

4. Oversight of the use of powers

Postal Packets and Telecommunications Messages (Regulation) Act 1993

Section 8 of the 1993 Act provides that the government can designate a High Court judge for the purposes of the 1993 Act (the Designated Judge). The Designated Judge must keep the operation of the 1993 Act under review and ascertain whether its provisions are being complied with.

The Designated Judge reports to the Irish Prime Minister (the Taoiseach) periodically and can investigate any case in which an authorisation of interception has been given. If the Designated Judge informs the Minister for Justice that a particular authorisation of interception should not have been given, should be cancelled or should not have been extended, the Minister for Justice shall inform the Minister and cancel the authorisation.

In addition, any contravention of the 1993 Act is subject to investigation by the complaints referee (a judge of the Circuit Court, District Court or a barrister or solicitor of at least 10 years' standing) (the Complaints Referee), under Section 9 of the 1993 Act. Where a person believes that a communication has been intercepted, they can apply to the Complaints Referee for an investigation into whether an authorisation of interception was in force and if so, whether there has been any contravention of the provisions of the 1993 Act. If there has been (i) a contravention; or (ii) a contravention which the Complaints Referee deems an offence, but not a serious offence, and the Complaints Referee refers the complaint to the Designated Judge who agrees; the Complaints Referee will notify the applicant and report their findings to the Taoiseach. The Complaints Referee may also:

i. quash the authorisation;
ii. direct the destruction of any copy of the intercepted communication; or
iii. recommend the payment of a specified sum of compensation to the applicant.

If there was no authorisation of interception or no contravention of the authorisation of interception, the Complaints Referee must inform the applicant of this.

A contravention of the provisions or conditions of the 1993 Act will not of itself render the authorisation of interception invalid or constitute a cause of action.

Criminal Justice (Surveillance Act) 2009

Where a person believes that they may be the subject of an authorisation or approval under Section 7 or 8 (urgent surveillance or tracking devices only, not regular authorisations) of the 2009 Act, they can apply to the Complaints Referee for an investigation into whether an authorisation or approval was granted and if so, whether there has been a relevant contravention of the 2009 Act. If there has been a contravention, the Complaints Referee will notify the applicant and report their findings to the Taoiseach. The Complaints Referee may also:

i. quash the authorisation or reverse the approval;
ii. direct the destruction of the written record of the approval and any material obtained;
iii. recommend the payment of a specified sum of compensation to the applicant; and
iv. report the matter to the Garda Síochána Ombudsman Commission or the Minister for Justice as appropriate.

Ireland

If there was no authorisation or approval, or no contravention of the authorisation/approval, the Complaints Referee must inform the applicant of this.

Under Section 11(9) of the 2009 Act, a relevant contravention which is not material will not of itself render the authorisation or approval invalid.

Most search warrants are issued by a District Court Judge or a Peace Commissioner. The judge or commissioner must consider the sworn information and, acting judicially, satisfy themselves that the requirements for the issue of a warrant under the relevant Act are fulfilled. However, in a small number of cases a warrant may be issued by a senior officer of the Garda Síochána.

Generally, Disclosure Orders are issued by a District Court Judge who must consider the sworn information and, acting judicially, be satisfied that the requirements for the issue of a Disclosure Order under the relevant Act are fulfilled.

Communications (Retention of Data) Act 2011

Section 1 of the 2011 Act defines 'designated judge' as a judge of the High Court designated under Section 8 of the 1993 Act. Section 12 of the 2011 Act provides that the Designated Judge must keep the operation of the 2011 Act under review and ascertain whether its provisions are being complied with. The Designated Judge reports to the Taoiseach periodically and can investigate any case in which an authorisation of interception has been given.

In addition, a contravention of the provisions of Section 6 (Disclosure Requests) under the 2011 Act will not of itself render the Disclosure Request invalid or constitute a cause of action.

Under Section 10 of the 2011 Act, where a person believes that data relating to them in the possession of a Licensed Operator has been accessed following a Disclosure Request, they can apply to the Complaints Referee for an investigation into whether a Disclosure Request was in force and if so, whether there has been any contravention of the provisions of Section 6 of the 2011 Act. If there has been a contravention, the Complaints Referee will notify the applicant and report their findings to the Taoiseach. The Complaints Referee may also:

i. direct the destruction of the relevant data and any copies thereof; and
ii. recommend the payment of a specified sum of compensation to the applicant.

If there was no Disclosure Request or no contravention of the Disclosure Request, the Complaints Referee must inform the applicant of this.

Censorship-related powers

1. Shut-down of network and services

There are two bodies empowered to shut down Vodafone's network and services; Ireland's Minister for Justice and Equality and the independent statutory body responsible for the regulation of the electronic communications sector in Ireland (ComReg).

Criminal Justice Act 2013

Sections 20 to 29 of the Criminal Justice Act 2013 permit the Minister for Justice and Equality, subject to certain conditions, to authorise the shut-down of mobile communication services in response to a serious threat. A serious threat is when an explosive or other lethal device will be activated by use of a mobile communication service and that activation will likely cause death, serious bodily harm or substantial property damage. In such circumstances, Vodafone could therefore be ordered to shut down its network by the Minister for Justice and Equality.

The Minister may only make such authorisation upon application having been made in writing by a member of the Garda Síochána not below the rank of Assistant Commissioner. The Minister may only then make the authorisation if they are satisfied that there are reasonable grounds for believing that a serious threat exists; there is a reasonable prospect that shutting the mobile communications service down would be of material help in averting that threat; and authorising the shut-down is necessary and proportionate in all the circumstances (including the importance of maintaining the availability of the mobile communications service and the effect of a cessation on users).

Section 24 provides that the Minister's authorisation shall remain in force for no longer than 24 hours and a mobile communication service shall be shut down for no longer than six hours.

European Communities (Electronic Communications Networks & Services) (Authorisation) Regulations 2011 SI 335/2011

Vodafone could have its authorisation to operate its network suspended or withdrawn by ComReg if it is in breach of the conditions attached to its authorisation.

Under Regulation 16(12) European Communities (Electronic Communications Networks and Services) (Authorisation) Regulations 2011 SI 335/2011, ComReg may take urgent interim measures to remedy certain types of situation. Those interim measures include requiring a network provider (such as Vodafone) to cease use of specified network apparatus with immediate effect.

Ireland

The type of situations in question relate to:

- when ComReg has evidence that a network provider has breached the conditions of its authorisation to provide an electronic communications network;
- its rights of use for radio frequencies or numbers; or
- specific obligations which represent an immediate and serious threat to public safety, public security or public health, or which will create serious economic or operational problems for other network providers or network users.

Regulation 17(1) enables ComReg to suspend or withdraw authorisation to provide an electronic communications network where there has been a serious or repeated breach by a network provider of the conditions attached to its authorisation. ComReg must first allow the network provider 28 days in which to make representations before effecting the suspension or withdrawal of authorisation.

2. Blocking of URLs and IP addresses

The government has no legal authority to order Vodafone to block URLs or IP addresses.

3. Power to take control of Vodafone's network

The government has no legal authority to control Vodafone's network subject to any such authority being introduced by emergency legislation passed in a state of emergency (during which the Constitution would be suspended on behalf of State security).

4. Oversight of the use of powers

There is no judicial oversight but every public law power is subject to judicial review so as to ensure that it is being used lawfully.

In addition, Regulation 4(1) of the European Communities (Electronic Communications Networks and Services) (Framework) Regulations 2011 SI 333/2011 states that a network provider (such as Vodafone) affected by a decision made by ComReg may appeal against that decision to the High Court within 28 days of being notified of that decision.

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes. There are a variety of legal powers which government and law enforcement agencies could potentially use to require a telecommunications operator to decrypt communications data.

The powers described (see 'Provision of real-time lawful interception assistance' above) would seem to be sufficiently broad that they could be used to issue a direction or authorisation requiring a telecommunications operator to decrypt communications data where the telecommunications operator has applied the encryption. However, for such a direction or authorisation to require the telecommunications operator to decrypt communications data, the direction or authorisation would need to very specifically refer to this. The recipient of such a direction or authorisation might argue that the decryption of communications data is beyond the scope of what was expressly intended by the statutory power giving rise to such direction or authorisation and/or that decryption was not technically feasible.

Disclosure Orders (see 'Disclosure of communications data' above) often include a provision stating that where the relevant information is not in legible form, the subject of the Order shall be required to give the password to the information to enable the LEA official to examine the information or produce the information in a form in which it is, or can be made, legible and comprehensible. As such, while the exact extent of the powers of an Irish LEA under a Disclosure Order will depend on the particular statutory provisions under which the Disclosure Order has been issued, it is possible that a Disclosure Order might require a telecommunications operator to decrypt communications data where the telecommunications operator has applied the encryption subject to the operator being satisfied that the decryption was in scope and technically feasible.

In addition, LEAs may obtain search warrants under approximately 200 different statutes. See 'Disclosure of communications data' above for a description of how they might be applied to the telecommunications operator. The extent of the powers of an Irish LEA under a search warrant will depend on the particular statutory provisions under which the warrant has been issued. There is no standard regime in relation to search warrants in Irish law and it is difficult to outline the exact obligations which all such warrants impose. However, it is possible that a search warrant might require the telecommunications operator to decrypt communications data where the

Ireland

telecommunications operator has applied the encryption.

Finally, Section 5 of the Criminal Justice Act 2006 (the **2006 Act**) states that where a member of the Garda Síochána has reasonable grounds for believing that there is evidence of, or relating to, the commission of arrestable offences (which are punishable by term of imprisonment of five years or more) (Arrestable Offences), they may take such steps as they reasonably consider necessary to preserve that evidence. Section 5(19) defines 'preserve', in relation to evidence as including any action to prevent the concealment, loss, removal, contamination or destruction of, or damage or alteration to, the evidence. This legal power could potentially be used by the Garda Síochána (where they have reasonable grounds for believing that there is evidence relating to the commission of Arrestable Offences contained in communications data) to require the telecommunications operator to decrypt communications data where the telecommunications operator has applied the encryption.

In addition, under the mutual assistance regime in Ireland (under the Criminal Justice (Mutual Assistance) Act 2008 and the Criminal Justice (Mutual Assistance) (Amendment Act) 2015), subject to compliance with the relevant procedures, some of the powers and/or remedies set out above (or similar powers or remedies) may be used by LEAs on behalf of foreign law enforcement agencies, including potentially to require the telecommunications operator to decrypt communications data where the telecommunications operator has applied the encryption.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

The powers summarised earlier in this chapter would seem sufficiently broad that they could be used to require a telecommunications operator to decrypt data carried on its networks as part of a telecommunications service or otherwise where the encryption has been applied by a third party, including equipment interference or other forms of assistance. However, for such a direction or authorisation to require a telecommunications operator to decrypt data where the encryption has been applied by a third party, the direction or authorisation would need to very specifically refer to this. The recipient of such an Order might argue that the decryption of communications data is beyond the scope of what was expressly intended by the statutory power and/or not technically feasible.

It is possible that the legal powers summarised earlier in this chapter and directly above at Question 1 (Disclosure Orders, Search Orders and preservation of evidence) could be used to require Vodafone to decrypt encryption that had been applied by a third party, including equipment interference or other forms of assistance.

In addition, under the mutual assistance regime in Ireland (see a more detailed description at Question 1 above) powers could potentially be used to require a telecommunications operator to decrypt communications data where the encryption has been applied by a third party, including equipment interference or other forms of assistance. However, again, this would be open to challenge by a telecommunications operator on the basis that it cannot be asked to do something that it lacks the technological capacity to do.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

We are not aware of any express legal prohibition on the telecommunications operator offering end-to-end encryption on its communication services. The telecommunications operator has positive obligations arising from Irish electronic communications and associated legislation, and its General Authorisation (ie its Irish telecoms regulatory authorisation) to protect the security and integrity of its networks, and the privacy and confidentiality of communications made using its network.

Such obligations are, however, subject to general law enforcement powers and remedies. As set out in response to Questions 1 and 2 above, existing law enforcement powers and/or remedies could be sufficiently broad to require that such practice is not applied in certain cases. However, the issue has not, to our knowledge, been tested in these specific circumstances in Ireland and could potentially be open to challenge.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

We are not aware of any reported judgments which have applied legislation predating the advent of commercial encryption to require a telecommunications service provider to decrypt data which was encrypted.

Italy

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

Real-time lawful interception forms part of the criminal investigation powers of the law enforcement agencies (LEAs), ie police, *carabinieri*, tax police and other authorised agencies: LEAs and intelligence agencies, as authorised by the competent judge or prosecutor.

Italian Criminal Procedure Code

Interceptions for criminal prosecution (Articles 266 to 271 of Italian Criminal Procedure Code): in the investigations related to certain crimes listed in Article 266 (eg crimes concerning arms and explosive substances, crimes committed with criminal intent punished with imprisonment up to five years, etc), the public prosecutor is entitled to ask the judge of the criminal investigation (GIP) to authorise real-time interceptions, if there are serious suspicions that the target is involved in the case and interception is necessary for the collection of evidence. In matters of urgency, the public prosecutor can directly authorise interceptions but the GIP shall validate such authorisation within 48 hours. Interception orders are granted for 15 days, renewable for further periods of 15 days (Article 267 of the Italian Criminal Procedure Code). In the case of investigations into organised crime (eg Mafia cases), interception orders are granted for 40 days, renewable for further periods of 20 days. Real-time interceptions can also be authorised for electronic and telematics communications (section 266 bis of the Italian Criminal Procedure Code).

Implementing provisions of the Criminal Procedure Code

Preventive interceptions by LEAs (Article 226 of Legislative Decree No. 271 of 1989): for the purpose of preventing specific crimes (eg committed by criminal associations and international terrorism organisations or for terrorism purposes through electronic devices), the Minister for Home Affairs or, where delegated by the latter, the Head of the Central and Interprovincial Department of LEAs or, in certain cases, the Head of the Anti-Mafia Investigation Department are entitled to ask the public prosecutor to authorise real-time interceptions. Interception orders are granted for 40 days, renewable for further periods of 20 days.

Law Decree No. 144 of 2005, as amended by Law No. 155 of 2005

Preventive interceptions by intelligence agencies (Article 4 of Law Decree No. 144 of 2005, as amended by Law No. 155 of 2005): the Prime Minister and, where delegated by the latter, the heads of Italian intelligence agencies (ie AISE and AISI) are entitled to ask the General Prosecutor before the Rome Court of Appeal to authorise interceptions for their scope of work, including enforcing national security. The General Prosecutor can authorise the requested interceptions through a reasoned decision. Interception orders are granted for 40 days, renewable for further periods of 20 days.

Given the legal framework described above, the relevant legislation regulating technical interception capabilities are the following:

Legislative Decree No. 259 of 2003 (Electronic Communications Code), prescribes that electronic communications service providers, including both Communications Service Providers (CSPs) and Internet Access Service Providers (ASPs), shall comply with any order for interceptions issued by judicial authorities; times and means are agreed with those authorities until approval of the repertoire referred in paragraph 2 of Article 96, not yet adopted.

On 15 December 2005, the Italian Privacy Authority, on the basis of the powers conferred to it by Legislative Decree No. 196 of 2003 (Data Protection Code) issued specific guidelines, prescribing to CSPs and ASPs a number of security measures with respect to mechanisms adopted by the CSPs and ASPs for dealing with judicial/LEAs' requests and delivering of intercepted products to LEAs, judicial authorities and intelligence agencies.

Electronic Communications Code

As a general rule, Article 96 of the Electronic Communications Code requires CSPs and ASPs to provide communications assistance and information to judicial authorities and LEAs for the purposes of criminal prosecution and national security. Pending the adoption of the intercept users' requirement (nicknamed *Repertorio*), provided for by Article 96(2) (a detailed specification of mandatory interception services and technical standards that has never been formally adopted, although a draft of it has been confidentially shared with telecom operators), technical capabilities are, from time to time, agreed between the CSPs/ASPs and public prosecutor/LEAs.

Italy

Italian Privacy Authority's Guidelines

The Italian Privacy Authority's Guidelines of 15 December 2005 require CSPs and ASPs to implement a number of organisational and security measures in respect of lawful interception and the exchange of information with LEAs, judicial authority and intelligence agencies.

The main security measures prescribed by the Italian Privacy Authority are the following:

a. Organisational aspects of security:
   - adoption of an organisational model to limit the knowledge of personal information processed;
   - appointment of the persons in charge of the data processing, including a control of the authentication systems and the access to data processed;
   - separation of data (accounting data from documentation data produced); and
   - strong authentication procedures, including also biometric verification.

b. Security of the information data flows from/to LEAs, judicial authority and intelligence agencies:
   - use of communications systems based on secure network protocols;
   - adoption of digital signatures to encode documents;
   - use of encoding systems based on digital signatures for all the communications with the judiciary authority and LEAs;
   - use of certified electronic mail (PEC); and
   - delivery of the documents by hand exclusively through persons appointed by the judiciary authority, keeping a register of the deliveries.

c. Protection of data processed for criminal prosecution/national security:
   - development of electronic means to ensure the control of the activities performed by each person in charge of the data processing with audit log registrations;
   - adoption of advanced encoding instruments for the protection of data during storage in the information technology systems of the CSPs/ASPs; and
   - limitation of retention of personal data for no longer than is strictly necessary to perform the order of the judicial authority providing for the cancellation of data immediately after the correct transmission to the judicial authority.

Recording of intercepted products has to be carried out by law enforcement monitoring facilities (LEMF) located in the building of the local/district prosecutor. However, in the case of interception of 'data' communications, the public prosecutor may order that the relevant interceptions be carried out by means of equipment owned by private companies or individuals (Article 268(3 bis) of the Italian Criminal Procedure Code) outside the prosecutor's building.

2. Disclosure of communications data

According to the relevant provisions of the Italian Criminal Procedure Code and Legislative Decree No. 271 of 1989, CSPs and ASPs can be required to provide LEAs (duly authorised by the judicial authority) with metadata relating to customers' communications within a criminal investigation as follows:

a. **Seizure of data in the possession of CSPs/ASPs within criminal proceedings** (Article 254 of Italian Criminal Procedure Code): The judicial authority has the power to order the seizure of any information that CSPs possess, including metadata, voicemail or an unread email in an inbox relating to customers.

b. **Access to customers' data by LEAs** (Article 226(4) of Legislative Decree No. 271 of 1989): For the purpose of preventing crimes by criminal associations and international terrorism organisations or crimes committed for terrorism purposes through electronic devices, the Minister for Home Affairs or, where delegated by the latter, the LEAs' Head of Regional Department or, in certain cases, the Head of the Anti-Mafia Investigation Department are entitled to ask the public prosecutor to order CSPs/ASPs to trace telephony and data communications and to authorise access to data relating to such communications and to any other relevant information stored by CSPs.

According to Article 96 of the Electronic Communications Code, CSPs and ASPs can be required to provide LEAs with information and metadata relating to customers in respect of the retention period established in Article 132 of the Data Protection Code (Legislative Decree No. 196/2003 and subsequent amendments).

According to the relevant provisions of the Italian Criminal Procedure Code, Legislative Decree No. 271 of 1989 and Electronic Communications Code, CSPs and ASPs can be required to provide LEAs (duly authorised by the judicial authority) with communications data stored in their database.

In addition, Article 55 of the Electronic Communications Code sets forth the obligation for CSPs and ASPs to provide the Minister of Internal Affairs with a list of all their customers or purchasers of pre-paid

Italy

mobile traffic. The judicial authorities can have access to such list for the performance of their duties.

Furthermore, according to Law No. 124 of 2007 on the reorganisation of the intelligence agencies, CSPs/ASPs can be required to cooperate with and provide access to their archives to intelligence agencies. This obligation has been recently clarified by the Prime Minister's Decree of 24 January 2013 on cyber security, which directly refers to this law. The Decree states that CSPs/ASPs are required to cooperate with intelligence agencies (AISE and AISI) and the National Security Department (DIS) according to their respective competences as set out by Law No. 124 of 2007, on the basis of specific operational agreements, in the interest of national security: ie in order to protect the independence, integrity and security of the Italian Republic from any internal or external subversive activity and criminal or terrorist attack. Furthermore, CSPs and ASPs shall provide information to and allow AISE, AISI and DIS to access their databases.

Finally, Law Decree No. 7 of 2015, as amended by Law No. 43 of 2015 on urgent measures against terrorism, as well as Law Decree No. 210 of 2015, as amended by Law No. 21 of 2016, introduce data-specific retention requirements for CSPs and ASPs, such as Vodafone.

3. National security and emergency powers

There are a number of provisions allowing the government to take over the management of networks in cases of emergency, such as disaster relief, search and rescue, public protection and national security. Among such provisions, below are the most relevant:

a. Article 11 of Ministerial Decree of 24 January 2013;
b. Article 73 of the Electronic Communications Code;
c. Article 2 of TULPS (Reformed Law on Public Security); and
d. Article 5.2 of Law No. 225 of 1992 on the Civil Protection Service.

Article 11 of the Ministerial Decree of 24 January 2013 provides that CSPs and ASPs must cooperate with the management of a cyber crisis, helping to restore network and communications systems in the event of failure.

Article 73 of the Electronic Communications Code establishes that, in the case of a severe network crash, the Ministry of Communications is entitled to set forth the measures needed for guaranteeing the availability of the public phone network. CSPs and ASPs must implement all the necessary measures for guaranteeing nonstop access to emergency services.

According to Article 2 of TULPS, the Prefect, in urgent situations or state of emergency, is entitled to adopt all the necessary decisions for protecting public order and public security.

According to Article 5.2 of Law No. 225 of 1992 on the Civil Protection Service, after the state of emergency has been declared, the Head of the Civil Defence Department can issue decrees with respect to, among other things, the restoring of strategic network infrastructures.

4. Oversight of the use of powers

In addition to the above, Article 98(3) and Article 32 of the Electronic Communications Code set out sanctions for CSPs/ASPs that do not comply with specific obligations to cooperate with judicial authorities and LEAs in relation to interception operations (eg fines and licence waiver).

In the case of seizure of communications data (eg historical traffic data, communications content) carried out within criminal proceedings, the authorisation and control of the GIP is necessary on the basis of the public prosecutors' request.

The activity of the intelligence agencies is directly monitored by the Prime Minister and by COPASIR, a special parliamentary committee whose function is to systematically ensure that Italian intelligence agencies operate in compliance with the Constitution and the law.

The judiciary plays no role in the execution of the operational agreements between the intelligence agencies and the CSP/ASP, or in the access operations. However, such agreements are notified to the DIS, and COPASIR is annually informed on the number of accesses to these databases.

In order to have access to communications data (eg historical traffic data, communications content), intelligence agencies need the authorisation of the General Prosecutor before the Court of Appeal.

Italy

Censorship-related powers

1. Shut-down of network and services

Legislative Decree No. 259 of 2003 (Electronic Communications Code)

Under Article 96 of the Electronic Communications Code, communications service providers (such as Vodafone) must comply with the requests of the competent judicial authority where this is for the purposes of justice. A list of the type of activities that communications service providers may be required to perform is contained in the s.c. 'Listino', adopted with Ministerial Decree No. 14120 of 26 April 2001, pursuant to Article 96(2) of the Electronic Communications Code. Such activities include shutting down the network or some service in a specified area.

Law No. 124 of 2007

Article 13(1) of Law No. 124 of 2007 establishes a general principle whereby communications service providers (such as Vodafone) are required to cooperate with the government intelligence agencies (ie DIS, AISE and AISI) if requested within their institutional scope of work.

The law does not include specific provision allowing – but nor does it prevent – intelligence agencies to interfere with communications network operation without previously requesting their cooperation.

Decree of the Prime Minister of 24 January 2013

The Decree of the Prime Minister of 24 January 2013 has established the guidelines to ensure cyber security and national security and confirms the crucial role played by 'ad hoc agreements' with communications service providers in Article 7, paragraph 5.

However, according to Article 11, all communications service providers (including Vodafone) have to cooperate in cyber crisis management, restoring the functionality of systems and networks under their control and to provide information to and allow AISE, AISI and DIS to access their databases in accordance with Law 124 of 2007. Based on such provision, there appears to be some areas where, even without a legally binding agreement, communications service providers must cooperate with the public entities for a prompt response to the crisis. The specific cooperation requested of the communications service providers is determined on a case-by-case basis.

The regulatory framework designed by Law No.1 24 of 2007 (as amended by Law No. 133 of 2012) gives a central role to the Prime Minister and to the acts that he can issue based on Article 1, paragraph 3.

Criminal Procedure Code

Other forms of cooperation – the content of which is not previously determined – may also be imposed by the judicial authorities and the judicial police pursuant to Article 348, paragraph 4 of the Criminal Procedure Code.

2. Blocking of domain names and IP addresses

Law No. 269 of 1998

Under Article 14-quater of Law No. 269 of 1998, as amended by Law No. 38 of 2006, communications service providers must implement filtering instruments and related technological measures to prevent access to websites containing content featuring child sex abuse. Such filtering instruments and related technological solutions are set by the Ministerial Decree of 8 January 2007 and include the blocking of URLs and IP addresses. The Ministry of Interior includes a department responsible for indicating the websites that must be blocked by communications service providers.

Law No. 296/2006

The Agency of State Monopolies (AAMS, Agenzia delle dogane e dei Monopoli) is responsible for combatting illegal gambling, and it can adopt specific orders forcing communications service providers (such as Vodafone) to implement technological measures that prevent access to illegal gambling websites, such as DNS blocking. The list of illegal gambling sites is provided and regularly updated by the Agency.

Legislative Decree No. 70 of 2003 (E-Commerce Decree)

According to Articles 14(3), 15(2) and 16(3) of the E-Commerce Decree, the judicial or administrative authority having controlling functions is entitled to order internet service providers (such as Vodafone) to immediately stop violations that are being committed on the internet.

Italian Criminal Procedure Code (Royal Decree No. 1398 of 1930)

According to Article 321 of the Italian Criminal Procedure Code, in the case of a criminal prosecution, the judicial authority may, at the public prosecutor's request, order the seizure of a thing (for example, a website) related to the crime, when such a thing is liable to aggravate the crime's consequences or to determine the commission of other crimes. In urgent cases, the judge's order may follow an act of seizure, provided it is within 48 hours of the act taking place.

Italy

3. Power to take control of Vodafone's network

Law No. 124 of 2007

Depending on the terms of the agreement between the intelligence agency and communications service provider, a communications service provider may be required to hand over control of its network to the intelligence agency in the interests of national security, with the authorisation of the Prime Minister or the judge. Please refer to 'Shut-down of network and services' above.

4. Oversight of the use of powers

E-Commerce Decree

Depending on the authority issuing the order, there could be either judicial or administrative oversight of an authority's use of its powers under the E-Commerce Decree.

Electronic Communications Code

A request made to a communications service provider to perform one of the activities listed in the 'Listino' must be made by a competent judicial authority. As a consequence, the exercise of the public powers requesting that cooperation is subject to judicial scrutiny.

Law No. 269 of 1998

The list of websites to be blocked by communications service providers under Law No. 269 of 1998 is maintained by a specific department of the Ministry of Interior. The courts do not have the power to review the Ministry's use of its powers in this respect.

Law No. 296 of 2006

Communications service providers (such as Vodafone) can receive specific communications by the Agency of State Monopolies aimed at removing the filter blocking the access to a given website. The list of the illegal gambling site is provided and regularly updated by the Agency.

Italian Criminal Procedure Code (Royal Decree No. 1398 of 1930)

The order is made by a judicial authority and therefore is subject to judicial review.

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Under Italian law, the government has no express legal power to require a telecommunications operator to decrypt communications data. However, there are a number of legal obligations mentioned above (see 'Provision of real-time lawful interception assistance' and 'Disclosure of communications data') that entail the duty of CSPs to provide authorities with cleartext data, which in practice will include the obligation to decrypt data where Vodafone has control over the encryption and/or has the possibility to access cleartext data.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

Italian law does not expressly provide for the government's legal power to require a telecommunications operator to decrypt data carried on its networks as part of a telecom service where the encryption has been applied by a third party. However, as highlighted in Question 1 above, under Article 96 of the Electronic Communications Code, in the case of legal interception arranged by the judicial authority, a telecommunications operator has an obligation to provide the competent authority with access to cleartext data, in order to allow the hearing of the content and conversations ; although there is no obligation if the contents are related to OTT.

Italy

Therefore, although the government has no legal authority to require a telecommunications operator to decrypt data carried on its networks, in the context of legal interception, the judicial authority can order a telecommunications operator to provide the relevant data in clear. Practically speaking, the legal obligations mentioned in Question 1 can only require a CSP to provide cleartext data where the CSP has actual control over the encryption and/or has the possibility to access the cleartext data.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

Under Italian law, there are no express provisions prohibiting a telecommunications operator from offering end-to-end encryption on its communications services. However, as highlighted in Questions 1 and 2 above, with respect to the obligations under Article 96 of the Electronic Communications Code, in the case of legal interception arranged by the judicial authority, a telecommunications operator has an obligation to provide cleartext data to the relevant authorities, in order to enable lawful interception. In light of that legal obligation, in our view a telecommunications operator would not be able to offer end-to-end encryption to its users where the ability to provide cleartext data would be outside of its control.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

We are not aware of any examples.

Kenya

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

The National Intelligence Service Act (Act No. 28 of 2012)

The National Intelligence Service Act (Act No. 28 of 2012) (the **NIS Act**) allows the Director-General (the DG) of the National Intelligence Service (NIS) (pursuant to Section 36) to monitor or otherwise interfere with the privacy of a person's communications.

The Security Laws (Amendment) Act No. 19 of 2014 (the **SLA Act**) amended the NIS Act by repealing the entire Part V and substituting it with a new part. Pursuant to the 'new' Section 42(2) where the DG has reasonable grounds to believe that a covert operation is necessary to enable the NIS to deal with any threat to national security or to perform any of its functions, the DG may, subject to any guidelines approved by the NIS Council, issue a written authorisation valid for 180 days to an officer of the NIS. No guidelines by the NIS Council in relation to the written authorisation have been issued yet.

Under Section 42(3)(a) and (b) such written authorisation is sufficient authorisation for officers of the NIS to conduct an operation and the authorisation may be served on any person required to assist the NIS or facilitate the covert operation or investigations to be undertaken.

The written authorisation may by virtue of Section 42(3)(c) authorise any member of the NIS to obtain any information, material, record, document or thing and, for that purpose, such a member may be authorised to:

a. enter any place, or obtain access to anything;
b. search for or remove or return, examine, take extracts from, make copies of or record in any other manner the information, material, record, document or thing;
c. monitor communication;
d. install, maintain or remove anything; or
e. take all necessary action, within the law, to preserve national security.

Provided that the written authorisation permits any of these actions, the authorisation is to be accompanied by a warrant issued by the High Court.

The Prevention of Terrorism Act (Act No. 30 of 2012)

Section 36(1) and (2) of The Prevention of Terrorism Act (Act No. 30 of 2012) (the **PT Act**) allows a police officer (subject to consent from the Inspector-General or the Director of Public Prosecutions) to apply for an interception of communications order.

Section 36(3) of the PT Act allows for the issuance of an interception order that requires a communications service provider to intercept and retain a specified communication of a specified description received or transmitted or about to be received or transmitted by the communications service provider, or to 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 and to remove and retain such device.

The SLA Act introduced Section 36A to the PT Act which permits National Security Organs to intercept communication for the purposes of detecting, deterring and disrupting terrorism in accordance with procedures to be prescribed by the Cabinet Secretary responsible for internal security.

The Mutual Legal Assistance Act (Chapter 75A Laws of Kenya)

Pursuant to The Mutual Legal Assistance Act (Chapter 75A Laws of Kenya) (the **MLA Act**), a requesting state may make a request to Kenya for the interception and immediate transmission of telecommunications, or the interception, recording and subsequent transmission of telecommunications. Under Section 27 of the MLA Act, for the purpose of a criminal investigation, Kenya may, in accordance with the provisions of this Act and any other relevant law, execute such a request from a requesting state for the interception and immediate transmission of telecommunications, or the interception, recording and subsequent transmission of telecommunications.

Section 32(1) of the MLA Act states that a request may be made to Kenya from a requesting state for deployment of covert electronic surveillance.

Kenya Information and Communications Act (Chapter 411A, Laws of Kenya)

The statutes mentioned above should be considered in the context of Section 31 of the Kenya Information and Communications Act (Chapter 411A, Laws of Kenya) (the **KIC Act**) which makes it an offence punishable by conviction with a fine not exceeding 300,000

Kenya

shillings, or by imprisonment for a term not exceeding three years, or by both where a licensed telecommunications operator who otherwise than in the course of their business:

- intercepts a message sent through a licensed telecommunications system;
- discloses to any person the contents of a message intercepted; or
- discloses to any person the contents of any statement or account specifying the telecommunications services.

Section 93 of the KIC Act obliges the Communications Authority (the CA) to implement any information access and disclosure restrictions pursuant to Article 35 of the Constitution which makes access to information including information held by the state a fundamental right.

Kenya Information and Communications (Consumer Protection) Regulations 2010

Further, Regulation 15(1) of the Kenya Information and Communications (Consumer Protection) Regulations 2010 requires that, subject to the provisions of the KIC Act or any other written law, a licensee (licensed under the **KIC Act**) does not monitor, disclose, or allow any person to monitor or disclose, the content of any information of any subscriber transmitted through the licensed system by listening, tapping, storage, or other kinds of interception or surveillance of communications and related data.

Section 31 of the KIC Act and Regulation 15(1) of the Kenya Information and Communications (Consumer Protection) Regulations 2010 is however qualified by Section 93 of the KIC Act which allows for disclosure of information in accordance with the provisions of Article 35 of the Constitution.

2. Disclosure of communications data

Kenya Information and Communications Act (Chapter 411A, Laws of Kenya) (KIC Act)

Section 89(1) of the KIC Act provides the powers to enter and search premises, and extends to obtaining any article or thing. These powers extend to obtaining data related to customer communications. A court is permitted to grant a search warrant to enable entry of any premises and to search, examine and test any station or apparatus, or obtain any article or thing.

Kenya Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations 2013

Regulation 10(1) prohibits the disclosure of the registration particulars of a subscriber without the subscriber's written consent except where the information is required:

a. for the purpose of facilitating the performance of any statutory functions of the CA;
b. in connection with the investigation of any criminal offence;
c. for the purpose of any criminal proceedings; or
d. for the purpose of any civil proceedings under the KIC Act.

The National Intelligence Service Act (Act No. 28 of 2012) (NIS Act)

Section 42 of the NIS Act permits the DG to issue a written authorisation which may be served on any person required to assist the NIS or facilitate a covert operation or investigation. The written authorisation, accompanied by a warrant, may also permit any member of the NIS to access any place and obtain access to anything and examine, record and take copies or extracts of any information, material, record, documents or thing.

The Mutual Legal Assistance Act (Chapter 75A Laws of Kenya) (MLA Act)

Section 28 of the MLA Act allows a requesting state to make a request for legal assistance in accordance with Kenyan law for the provision of data relating to customer communications.

The Anti-Money Laundering Act (Chapter 59B)

Section 103 of the Proceeds of Crime and Anti-Money Laundering Act (Chapter 59B) authorises the police to apply for production orders where a person has been charged with, or convicted of, an offence and a police officer has reasonable grounds for suspecting that any person has possession or control of:

a. a document relevant to identifying, locating or quantifying property of the person, or to identifying or locating a document necessary for the transfer of property of such person; or
b. a document relevant to identifying, locating or quantifying tainted property in relation to the offence, or to identifying or locating a document necessary for the transfer of tainted property in relation to the offence.

The police officer may make an ex parte application with a supporting affidavit to a court for an order against the person suspected of having possession or control of a document of the kind referred to, to produce it.

3. National security orders and emergency powers

The National Intelligence Service Act (Act No. 28 of 2012) (NIS Act)

As described above, pursuant to Section 42(2) of the NIS Act where the Director-General has reasonable grounds to believe that a covert operation under this Section is required to enable the NIS to investigate or deal with any threat to national security or to perform any of its functions, they may, subject to the guidelines approved by the Council, issue a written authorisation requiring any person to facilitate or assist the NIS in its investigation

Kenya

and, when accompanied by a warrant, to monitor or otherwise interfere with the privacy of a person's communications to enable the investigation of any threat to national security.

The Constitution of Kenya 2010

Under Articles 58 and 132(4) of the Constitution, the President may declare a state of emergency, and any legislation enacted or other action taken in consequence of the declaration shall be effective only prospectively and not longer than 14 days from the date of declaration, unless the National Assembly resolves to extend the declaration. After the declaration of a state of emergency, the government would have broad powers, which could extend to a range of actions in relation to Vodafone's network and/or customer communications.

The Preservation of Public Security Act (Chapter 57)

Section 3 of the Preservation of Public Security Act (Chapter 57) (the **PPS Act**) states that the President may publish a declaration under the PPS Act when it appears that such a declaration is necessary for the preservation of public security. Section 4(1) and (2) state that in such instances, the President shall have the power to make regulations for *inter alia* the censorship, control or prohibition of the communication of any information or of any means of communicating.

4. Oversight of the use of powers

The oversight role of the judiciary pursuant to the NIS Act has been further limited by the amendments to the NIS Act made by the SLA Act. With the amendments, a written authorisation by the DG is sufficient to require a person to facilitate or assist a covert operation or investigation by the NIS. As indicated above, a warrant is, however, necessary where any such written authorisation permits a member of the NIS to obtain information, monitor communication or install, maintain or remove anything.

Further, Section 65 of the NIS Act was amended by the SLA to provide that the National Assembly rather than the Parliament of Kenya (through the relevant committee) has oversight authority over all the workings of the NIS pursuant to Article 238(2) of the Constitution of Kenya (2010).

Regarding powers granted to the President in a state of emergency, pursuant to Article 58(5) of the Constitution of Kenya, the Supreme Court may decide on the validity of a declaration of a state of emergency, any extension of a declaration of a state of emergency and any legislation enacted, or other action taken, in consequence of a declaration of a state of emergency.

Censorship-related powers

1. Shut-down of network and services

Constitution

There is no clear legislation on this issue. Pursuant to Article 58 and Article 132(4) of the Constitution of Kenya, the President may declare a state of emergency. After a declaration of a state of emergency, the government has broad powers. It is feasible that such powers could extend to ordering the shut-down of Vodafone's network and/or certain of its services. Any action or legislation taken in consequence of a declaration of a state of emergency is effective for no longer than 14 days from the date of declaration, unless the National Assembly resolves to extend the declaration.

In the recent case of *Royal Media Services Limited vs. The Hon. Attorney General, The Minister of Information and Broadcasting and the Communications Commission of Kenya [Petition No. 59 of 2013 High Court of Kenya]*, the petitioner (a broadcasting station called Royal Media Services Limited) had its transmitters disabled and shut down by the government.

The Kenya Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations 2012

Under Regulations 11 and 12 of The Kenya Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations 2012, telecommunications services must be suspended with respect to subscribers who fail to register their details. Upon expiry of the 90-day suspension period, a subscriber's individual access to the telecommunications service is deactivated.

The Preservation of Public Security Act (Chapter 57)

The President may make a declaration for the preservation of public security under Section 3 of the Preservation of Public Security Act (Chapter 57) (the PPS Act). In the period during which such a declaration is in force, the President bears power to make regulations for *inter alia* the censorship, control or prohibition of the communication of any information or of any means of communicating.

Kenya

2. Blocking of URLs and IP addresses

See Section 1 'Shut-down of network and services' above. It is plausible that, were a state of emergency to be declared or a declaration for the preservation of public security be made by the President, the government might use its emergency powers to order Vodafone to block specified URLs, IP addresses or IP ranges.

3. Power to take control of Vodafone's network

See Section 1 'Shut-down of network and services' above. It is plausible that, were a state of emergency to be declared or a declaration for the preservation of public security be made by the President, the government might use its emergency powers to take control of Vodafone's network.

4. Oversight of the use of powers

Constitution

Under Article 58(5) of the Constitution of Kenya, the Supreme Court may decide whether a declaration of a state of emergency is valid. The Supreme Court may also preside over whether the extension of a declaration of a state of emergency beyond 14 days and any legislation enacted in consequence of a declaration of a state of emergency is valid.

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes. The extent to which such regulations may permit National Security Organs (NSOs) to require encrypted data to be decrypted is not set out in the Act. However, it would not, in the context of modern communication, be astounding for the regulations to extend that far.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

While there is no specific Kenyan law on investigation of electronic data protected by encryption, the powers granted to National Security Organs under the NIS Act and POTA are far-reaching.

As indicated above, under Section 42 of the NIS Act, Sections 35, 36 and 36A of the POTA and Sections 27 and 28 of the MLA, NSOs have the power to intercept communication and require cooperation by CSPs. These powers include, in the case of the NIS, the power, albeit under warrant, to obtain access to anything in the custody of a person required to assist an investigation and to take all necessary action, within the law, to preserve national security. These general powers could extend to requiring a telecommunications operator to decrypt communication transmitted through its network by an 'over the top' communications service provider, should the telecommunications operator have the ability to do so.

The scope of what an NSO could achieve under these powers is untested in Kenyan Courts.

However as an indication of the general school of thought, a challenge to the constitutionality of Section 42 of the NIS Act and Section 36A of the POTA at the Constitutional and Human Rights Division of the High Court in *Coalition for Reform and Democracy (CORD) & 2 others v Republic of Kenya & 10 others* (2015) eKLR was defeated on the basis that the powers granted to NSOs under those sections were justified, would serve a genuine public interest and were not unduly restrictive in view of the nature of terrorism and sophistication of modern communication.

Please also note that Condition 14 of the Network Facilities Provider Tier 2 Licence No. TL/NFP/T2/00054 dated 14 September 2009 imposes a duty on the CSP to keep information obtained in the course of its business from any of its subscribers confidential. However clause 14.3 exempts CSPs from the obligation to keep such information confidential for the purpose of law enforcement, national interest or pursuant to any law.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

There is no clear legislation on this aspect. Please note however that following the reasoning of the court in *Coalition for Reform and Democracy (CORD) & 2 others v Republic of Kenya & 10 others* (2015) eKLR, it would appear that the courts would likely interpret the law to err on the side of caution, more so due to the recurrence of terrorist attacks. It remains to be seen if the courts will view the obligation to assist to also extend to an obligation not to inadvertently block attempts by NSOs to access encrypted information.

Kenya

In any case, note that CSPs are required to submit quarterly and annual reports to the Communications Authority of Kenya under the Kenya Information and Communications (Compliance Monitoring, Inspections and Enforcement) Regulations 2010. If the encryption service prevents the CSP from meeting its reporting or other obligations under the law and under the licence, then it is likely to be viewed as a breach of the conditions of the licence and the law.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

Kenyan law on encryption and access to encrypted data is limited. However, being a common law jurisdiction, the courts look to decisions made in other common law jurisdictions as persuasive authorities that give guidance in reaching a decision. As such, the global treatment of the obligation to decrypt data and local prevailing circumstances may influence the decision reached.

The Kenyan Judicature Act at Section 3 incorporates English Statutes of General Application passed on or before 12 August 1897 into Kenyan law, unless specifically repealed by Kenyan law, provided that the statutes only apply in so far as the circumstances of Kenya and its inhabitants permit, and subject to such qualifications as those circumstances may render necessary.

Lesotho

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

Communications Act 2012

Section 44(1)(f) of the Communications Act 2012 (**Communications Act**) states that a person may not intercept communications or messages unless authorised by a court of competent jurisdiction. Therefore, the government does not have the legal authority to require Vodafone to intercept individual customer communications or messages without a court order.

In Lesotho, there appear to be no specific laws that grant law enforcement agencies with legal powers to allow direct access into a communication service provider's network outside the operational control or oversight of the service provider.

2. Disclosure of communications data

Telecommunications Authority Regulations 2001

Regulations 32(1) and (2) of the Telecommunications Authority Regulations 2001 state that no person while engaged in the operation of a telecommunications service may disclose information about a customer, unless disclosure is required in connection with the investigation of a criminal offence or for the purpose of criminal proceedings.

Criminal Procedure and Evidence Act 1981

According to the Criminal Procedure and Evidence Act 1981 (Sections 46 to 49), a judicial officer may issue a warrant authorising the search of a property, if he or she has a reasonable suspicion that there is anything on the property that amounts to evidence of an offence, or which will be used in a criminal offence. However, a policeman/woman (with the rank of warrant officer and above) may conduct the search without a warrant if he or she believes that first obtaining the warrant will defeat the purpose of the search.

The Prevention of Corruption and Economic Offences Act No. 5 of 1999

The Prevention of Corruption and Economic Offences Act (**Act**) provides for the disclosure of information in connection with the investigation or prevention of corruption and economic offences. Section 8 of the Act states that the Director of Prevention of Corruption and Economic Offences may, by notice in writing, require any person to furnish, notwithstanding the provisions of any other enactment to the contrary, all information in his or her possession relating to the affairs of any suspected person, and to produce or furnish any document or certified true copy of any document relating to such suspected person, which is in the possession or the control of the person required to furnish the information.

Ombudsman Act 1996

The Office of the Ombudsman was established under Section 134 of the constitution of Lesotho, among other things, to investigate action taken by any officer or authority in the exercise of the administrative functions of that officer or authority in cases where it is alleged that a person has suffered injustice in consequence of that action.

Section 9 of the Ombudsman Act 1996 states that in the performance of his or her functions the Ombudsman will have the power 'to summon and subpoena in writing any person to produce any records in the custody, possession or control of that person, which the Ombudsman may deem necessary in connection with any inquiry before him; and for such purpose he shall have similar powers to those of a High Court Judge but subject to the same rules relating to immunity and privilege from disclosure as apply in High Court'.

3. National security and emergency powers

National Security Services Act No. 11 of 1998 (NSS)

Section 26 of the NSS states that 'The Minister may, on an application made by a member of or above the rank of Higher Intelligence Officer, issue a warrant authorising the taking of such action in respect of any property specified in the warrant as the Minister thinks is necessary to be taken in order to obtain information which: (a) is likely to be of substantial value in assisting national security services in discharging any of its function; and (b) cannot be reasonably obtained by any other means'.

Lesotho

Emergency Powers Order 1988

Section 5(3)(b) of the Emergency Powers Order 1988 (**Emergency Powers Order**) states that the Minister responsible for defence and internal security may, during a declared state of emergency, issue regulations (**Regulations**) that authorise the acquisition of any property in Lesotho, and take possession and control of such property. Section 5(3)(b) of the Emergency Powers Order has not been enacted to date. The Regulations are made by the Minister's office, but have to be issued in the Government Gazette to be generally enforceable. Any further processes detailing the right to access customer data and/or the network would presumably be set out in those Regulations.

4. Oversight of the use of powers

Interception of communications is only allowed if authorised by a court order, and the court, which has to be of competent jurisdiction, has discretion in this regard. The court will allow the interception of messages if it is reasonable and serves a lawful purpose.

Section 26(3) of the NSS provides that such 'a warrant shall not be issued unless: (a) it is signed by the Minister, or (b) in an urgent case where the Minister has expressly authorised its issue and a statement of that fact is endorsed on it, it is signed by the Director General or an office authorised by the Director General'.

State conduct will always be subject to the constitution of Lesotho, which guarantees freedom from arbitrary seizure of property and freedom from arbitrary searches. These rights can be limited where state security or public order (among other things) requires. Therefore, laws of general application that limit the rights in question, such as the Regulations that can be enacted in terms of the Emergency Powers Order, will be valid and enforceable, as long as the means (search or seizure) are proportional, or rationally related, to achieve the end result (state security or public order).

Censorship-related powers

1. Shut-down of network and services

Communications Act 2012

According to Section 20 of the Communications Act 2012 Vodafone may be prevented from providing all or some of its network or services in Lesotho if either the regulatory body, the Lesotho Communications Authority, revokes Vodafone's licence or the Minister issues an emergency suspension notice.

The Minister may only issue an emergency suspension notice if he or she has a reasonable basis to conclude that the continued operation by Vodafone of its network poses a substantial threat to national security or public order, and that there is no other way to forestall the danger. Section 20(3) states that the emergency order by the Minister must be in writing; set out the basis for the suspension; and remain in effect for no more than 72 hours unless extended by a court of competent jurisdiction.

2. Blocking of URLs and IP addresses

The government in Lesotho does not have the legal authority to order a network provider (such as Vodafone) to block URLs or IP addresses.

3. Power to take control of Vodafone's network

Emergency Powers Order 1988

Under Section 5(3)(b) of the Emergency Powers Order 1988, the Minister responsible for defence and internal security may, during a declared state of emergency, issue regulations that authorise the acquisition and taking into possession and control of any property or undertaking. A state of emergency may be declared by the King by proclamation in the Gazette when it is in the interests of public safety and public order. It is therefore possible that, during a declared state of emergency, the Minister might take control of Vodafone's network in Lesotho. No such regulations have been made to date.

4. Oversight of the use of powers

Communications Act 2012

Vodafone may appeal to the judicial courts on an urgent basis for relief before the 72-hour suspension starts if it feels that there is no proper basis for the Minister's suspension of its network or services.

Emergency Powers Order 1988

The conduct of the Minister responsible for making the regulations in a state of emergency pursuant to the Emergency Powers Order 1988 will always be subject to the constitution of Lesotho. The constitution of Lesotho upholds the freedom of its citizens from arbitrary seizure of property and arbitrary searches. These rights can, however, be limited where state security or public order (among other things) requires. Against that context, a regulation ordering the seizure of Vodafone's network would be valid and enforceable provided it is proportionate and rationally related to achieving its objective – namely that of maintaining state security and public order.

Lesotho

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Generally, the government of Lesotho does not have the legal authority to require a telecommunications operator to intercept communications without a court order (see earlier in this chapter under 'Provision of real-time lawful interception assistance').

Were a court to order a telecommunications operator to perform an interception on its network, there is nothing in the law to prevent the court from ordering a telecommunications operator to remove any encryption that it had applied in order to enable the interception.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

There is, currently, no legislation in Lesotho that would give government the legal authority to require a telecommunications operator to decrypt data carried on its networks, as part of a telecommunications service or otherwise, where encryption has been applied by a third party.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

There is no legislation which specifically governs encryption of data communication. Our understanding is that decryption is an integral part of data interception. We are, therefore, of the view that offering end-to-end decryption which we are unable to break would amount to flouting our statutory obligations if interception can be ordered.

We are of the view that the position would be different where a telecommunications operator customer accesses and downloads a third-party app via a third-party app store, because there would have been no positive action taken by a telecommunications operator in encrypting the data.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

There are no such examples in Lesotho.

Malta

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

Security Service Act

Under the Security Service Act (**Chapter 391**) of the Laws of Malta, the Security Service of Malta can obtain authorisation for interception or interference with communications by means of a warrant issued by the Minister responsible for the Security Service (the Minister).

Article 3 of Chapter 391 states that the function of the Security Service will be to protect national security, in particular against threats from organised crime, espionage, terrorism and sabotage, against the activities of agents of foreign powers and against actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means. Furthermore, the Security Service will act in the interest of the economic well-being of Malta and public safety, particularly in relation to the prevention or detection of serious crime.

Chapter 391 does not provide for a definition of 'serious crime'.

Chapter 391 defines 'interception' as 'in relation to a warrant, the obtaining possession of, disrupting, destroying, opening, interrupting, suppressing, stopping, seizing, eavesdropping on, surveilling, recording, copying, listening to and viewing of communications and the extraction of information from such communications'.

According to Chapter 391, following a request made by the Security Service, the Minister may issue a warrant authorising the taking of such action as is specified in the warrant in respect of any communications. The warrant must be issued under the hand of the Minister or in an urgent case where the Minister has expressly authorised its issue, and a statement of that fact is endorsed by the hand of a senior government official who is a Permanent Secretary or the Cabinet Secretary.

Warrants are generally valid for six months (if issued by the Minister) or two days (if not issued by the Minister). Warrants may be modified or cancelled by the Minister at any time. The Minister can also extend their validity for a further six months.

Electronic Communications Network and Services (General) Regulations

Under the conditions contained in the authorisation issued by the Malta Communications Authority to Vodafone pursuant to the Electronic Communications Networks and Services (General) Regulations (**SL 399.28**), Vodafone, as an authorised undertaking, has an obligation to comply with all requirements related to legal interception and data retention as may be established under the Electronic Communications (Regulation) Act (Chapter 399) or any other law.

To this date, no specific laws have been published in relation to the obligation of authorised undertakings to assist in implementing interception capabilities. However, authorised undertakings are required to assist law enforcement agencies, most notably the Security Service, in implementing interception capabilities on their networks and this is part of their authorisation conditions even though no specific law to this effect exists. Chapter 391 provides for warrants related to interception and not to any specific obligations on the network providers.

Article 86 of SL 399.28 states that the Malta Communications Authority will define the technical and operational requirements necessary to enable legal interception of electronic communications by the competent authorities in accordance with any law allowing and regulating such legal interception, provided that in doing so, the Malta Communications Authority will give reasons for the technical and operational requirements it defines and will seek to ensure that any expenses that undertakings may have to incur in order to meet any requirements it establishes are reasonable and justified.

Therefore, while no direct legal provision exists relating to the obligation of authorised undertakings to implement interception capabilities on their networks, the authorised undertakings have a legal obligation to fund the infrastructure used for such activities.

2. Disclosure of communications data

Processing of Personal Data (Electronic Communications Sector) Regulations

Disclosure of metadata is governed by Part II of the Processing of Personal Data (Electronic Communications Sector) Regulations (**SL 440.01**).

Disclosure of metadata is to be made by service providers of a publicly available electronic communications service or of a public communications network, in an intelligible form and only to the Police or the Security Service.

Malta

Regulation 20 of SL 440.01 provides for the disclosure of the following types of data which are traditionally considered metadata:

1. **Data necessary to trace and identify the source of a communication:**

a. concerning fixed network telephony and mobile telephony:
   - the calling telephone number; and
   - the name and address of the subscriber or registered user;

b. concerning internet access, internet email and internet telephony:
   - the user ID allocated;
   - the user ID telephone number allocated to any communication entering the public telephone network; and
   - the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication.

2. **Data necessary to identify the destination of a communication:**

a. concerning fixed network telephony and mobile telephony:
   - the telephone number or numbers dialled or called and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed; and
   - the name and address of the subscriber or registered user;

b. concerning internet email and internet telephony:
   - the user ID or telephone number of the intended recipient of an internet telephony call; and
   - the name and address of the subscriber or registered user and user ID of the intended recipient of the communications.

3. **Data necessary to identify the date, time and duration of a communication:**

a. concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

b. concerning internet access, internet email and internet telephony:
   - the date and time of the log-in and log-off of the internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the internet access service provider to a communication, and the user ID of the subscriber or registered user; and
   - the date and time of the log-in and log-off of the internet email service or internet telephony service, based on a certain time zone.

4. **Data necessary to identify the type of communication:**

a. concerning fixed network telephony and mobile telephony, the telephone service used; and

b. concerning internet email and internet telephony, the internet service used.

5. **Data necessary to identify users' communication equipment or what purports to be their equipment:**

a. concerning fixed network telephony, the calling and called telephone numbers;

b. concerning mobile telephony:
   - the calling and called telephone numbers;
   - the International Mobile Subscriber Identity (IMSI) of the calling party;
   - the International Mobile Equipment Identity (IMEI) of the calling party;
   - the IMSI of the called party;
   - the IMEI of the called party; and
   - in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

c. concerning internet access, internet email and internet telephony:
   - the calling telephone numbers for dial-up access; and
   - the digital subscriber line or other end point of the originator of the communication.

6. **Data necessary to identify the location of mobile communication equipment:**

a. the Cell ID at the start of the communication; and

b. data identifying the geographic location of cells by reference to their Cell IDs during the period for which communications data are retained.

According to Regulation 19 of SL 440.01, metadata is to be disclosed to the Police or the Security Service where such data is required for the investigation, detection or prosecution of a serious crime.

SL 440.01 defines 'serious crime' as any crime which is punishable by a term of imprisonment of not less than one year and, for the purposes of SL 440.01, includes the crimes mentioned in Articles 48(1)(d) and 49 of Chapter 399.

A request for data is to be made in writing and will be 'clear and specific', but if the data is urgently required, such a request is made orally; however, a written version of the request will be made at the earliest opportunity.

Regulation 18(1) of SL 440.01 provides that there is no legal obligation on providers of publicly available electronic communications services or of a public communications network to retain data revealing content of any communication.

Malta

Criminal Code

Furthermore, Article 355AD of the Criminal Code (Chapter 9) provides that any person who is considered by the Police to be in possession of any information or document relevant to any investigation has a legal obligation to comply with a request from the police to attend at a police station to give, as required, any such information or document, provided that no person is bound to supply any information or document which would incriminate them.

If information is provided in accordance with Article 355AD, the Police may, orally or by a notice in writing, require any person to attend at the police station, or other place indicated by them, to give such information and to produce such documents as the Police may require and if that person does attend the police station or place indicated to them, they will be deemed to have done so voluntarily. The written notice will contain a warning of the consequences of failure to comply, namely that the person will be guilty of a contravention punishable with detention and will be liable to be arrested immediately under warrant. The written notice may be served with urgency in cases where the interests of justice so require.

3. National security and emergency powers

Emergency Powers Act

Under the provisions of the Emergency Powers Act (Chapter 178), following a declaration by the President of Malta of a state of public emergency, the President of Malta, acting on the advice of the Prime Minister, may make such regulations as appear to him or her to be necessary or expedient for securing the public safety, the defence of Malta, the maintenance of public order and the suppression of mutiny, rebellion and riot, and for maintaining supplies and services essential to the life of the community, subject to the provisions of the Constitution of Malta. Such regulations (in accordance with Article 4(2) of Chapter 178) can include authorising taking possession or control on behalf of the government of any property or undertaking as well as providing for amending any law or suspending the operation of any law and for applying any law with or without modification. Such regulations will expire and cease to have effect after two months unless approved by a resolution of the House of Representatives (Article 6(1) of Chapter 178). These regulations may also be amended and revoked at any time by resolutions passed by the House of Representatives (Article 6(2) of Chapter 178).

Civil Protection Act

Under the Civil Protection Act (Chapter 411), in situations of emergency, disaster or other operation covered by Chapter 411, the Commander as appointed by Chapter 411 or the Director or highest ranking officer of the Assistance and Rescue Force may, among other things, order the immediate requisition of any movable or immovable thing, which is indispensably necessary in his or her judgement for any operation, subject to a right of compensation by the owner.

4. Oversight of the use of powers

Chapter 391 does not provide for judicial oversight. However, Chapter 391 establishes the post of a Commissioner who will keep under review, among other things, the exercise by the Minister responsible for the Security Service of powers to issue warrants.

The Information and Data Protection Commissioner is responsible for the compliance and enforcement of SL 440.01. Aggrieved persons can request his or her intervention. Any decision by the Information and Data Protection Commissioner may be contested in front of the Data Protection Appeals Tribunal.

The Information and Data Protection Commissioner may consult and seek advice of the Malta Communications Authority.

Subject to the Constitution of Malta, regulations issued under Chapter 178 can be revoked by resolution passed by the House of Representatives.

Malta

Censorship-related powers

1. Shut-down of network and services

Emergency Powers Act

Under Chapter 178 of the Emergency Powers Act, following a declaration by the President of Malta of a state of public emergency, the President, acting on the advice of the Prime Minister and subject to the provisions of the Constitution of Malta, may make such regulations as appear to him or her to be necessary or expedient for:

- securing the public safety;
- securing the defence of Malta; maintaining public order;
- suppressing mutiny, rebellion or riot; and/or
- maintaining supplies and services essential to the life of the community.

Under Article 4 of Chapter 178, such regulations can include authorising the government to take possession or control of property or undertakings; it is possible that this could include Vodafone's network equipment. It is feasible that, once in possession or control of Vodafone's network equipment, the government might use its powers to shut the network or services down.

2. Blocking of URLs and IP addresses

Emergency Powers Act

The government does not have the legal authority to block URLs or IP addresses. However, should the government take possession or control of Vodafone's network or services under the Emergency Powers Act, it would able to use that power to block URLs and IP addresses.

3. Power to take control of Vodafone's network

Emergency Powers Act

Under the Emergency Powers Act, the President has the power to control Vodafone's network where he or she has declared a state of public emergency. See 'Shut-down of network and services' above for more details about this power.

4. Oversight of the use of powers

Emergency Powers Act

Under Article 6(1) of the Emergency Powers Act, the regulations which the President is empowered to make under Article 4 expire after two months unless approved by a resolution of the House of Representatives. Under Article 6(2), such regulations may also be amended and revoked at any time by a resolution passed by the House of Representatives.

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

There is no express obligation at law through which the government can require a telecommunications operator to decrypt communications data where the telecommunications operator has applied the encryption itself, and Maltese law does not contain any specific provision regarding the decryption of telecommunications data.

However, Article 355AD of the Criminal Code, Chapter 9 of the Laws of Malta provides that:

4 Any person who is considered by the police to be in possession of any information or document relevant to any investigation has a legal obligation to comply with a request from the police to attend at a police station to give as required any such information or document:

Provided that no person is bound to supply any information or document which tends to incriminate him.

If the services provider can decrypt the said information, one may assume that the Police might also try to extend the applicability of Article 355AD in these situations. However, no legal precedent exists and it will be at the discretion of the court to accede or otherwise to a wide interpretation of this clause that may be attempted by the Police.

In addition to the above, Article 355Q of the same Criminal Code also provides that:

355Q. The Police may, in addition to the power of seizing a computer machine, require any information which is contained in a computer to be delivered in a form in which it can be taken away and in which it is visible and legible.

While it is noted that there is no explicit reference to decryption in this article, there is nothing stopping the Maltese Police from seizing servers containing encrypted communication data and subsequently asking the telecommunications operator to provide such data in a form which is 'visible and legible'. This assumes, however, that the Police would not focus on the obtaining of the information itself, but more specifically on the computer (or server) on which such information is stored.

Malta

Moreover, reference is also made to Article 19(1) and (2) of SL 440.01 Processing of Personal Data (Electronic Communications Sector) which, similarly to the Criminal Code, also provides that data retained by electronic communications service providers which is required by the Police or the Security Service for the prevention of serious crime will be provided to such authorities 'in an intelligible form and in such a way that it is visible and legible'. This also implies that the telecommunications operator may be required to decrypt data for such authorities.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

As explained above there are no Maltese law provisions which specifically deal with the decryption of data. In our view, because lawful interception (LI) is performed directly by government, if the government needed to decrypt encryption applied by a third party, it would approach the third party directly. We would not expect government to ask the telecommunications operator to assist with breaking the encryption when the telecommunications operator lacks the technological capacity to do so.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

Yes. Maltese law is completely silent on this matter and therefore we believe that this would not be in breach of the telecommunications operator's existing law enforcement obligations.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

There are no examples of this sort in the Maltese jurisdiction.

Mozambique

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

Decree No. 33/2001

Article 35 of the Regulation of the licensing and register for the providing of telecommunications services of public usage and establishing and usage of the public network of telecommunications (**Decree No. 33/2001** of 6 November) states that licensed providers are obliged to cooperate with the legal competent authorities regarding the legal interception of communications.

Under the Regulation, such interception will be made through the Regulatory Authority's duly credentialed members. It does not appear to provide a clear outline of the process; nor is there a law or decree that establishes one.

There appear to be no specific laws that grant law enforcement agencies the legal powers to allow direct access into a communications service provider's network without the operational or technical control of the communications service provider.

2. Disclosure of communications data

The Telecommunications Law

Article 68 of the Telecommunications Law (**Law No. 8/2004** of 21 July – the **Telecommunications Law**) states that the secrecy of the communications is guaranteed except in cases of criminal law and in the interests of national safety and the prevention of terrorism, criminality and organised delinquency.

3. National security and emergency powers

Except as already outlined above, the government agencies do not have any authority to invoke special powers to access a communications service provider's customer data and/or network on the grounds of national security.

Article 10 of the Telecommunications Law states that the government is responsible for the adequate coordination of the telecommunications services in emergency situations. In such situations, the government may issue a notice with mandatory instructions to the telecommunications operators. The Telecommunications Law does not provide a clear outline of the process; nor is there a law or decree that establishes the procedures.

4. Oversight of the use of powers

There does not appear to be any judicial oversight of the powers contained within this report, other than in cases of criminal law, which are overseen by judges sitting in the criminal courts of Mozambique.

Mozambique

Censorship-related powers

1. Shut-down of network and services

Decree No. 33/2001 of 6 November

Articles 10 and 37 of the Regulation of the licensing and register for the providing of telecommunications services of public usage and establishing and usage of the public network of telecommunications (Decree No. 33/2001 of 6 November) state that when a state of siege or emergency is declared, the Regulatory Authority has the power to cancel Vodafone's licence to provide its network and services in order to protect national security.

Separately, the Regulatory Authority may at any time suspend or revoke Vodafone's licence to provide its network and services if Vodafone breaches certain conditions set out in its licence. These conditions include Vodafone's requirement to cooperate with legally competent authorities in their interception requests.

2. Blocking of URLs and IP addresses

The government does not have legal authority to require Vodafone to block URLs or IP addresses.

3. Power to take control of Vodafone's network

Decree No. 33/2001

See 'Shut-down of network and services' above; the Regulatory Authority's power when a state of siege or emergency is declared could extend to taking control of Vodafone's network.

4. Oversight of the use of powers

There is no judicial oversight of the Regulatory Authority's execution of its powers.

Encryption and law enforcement assistance

Please note that since this legal analysis was undertaken, a new Telecommunications Law came into force on 3 August 2016.

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes. The statutory law in Mozambique does not expressly refer to encryption. The existing statutory obligations on a telecommunications operator are to:

- provide real-time lawful interception assistance under Decree No. 33/2001 (see 'Provision of real-time lawful interception assistance' above); and
- disclose communications data to competent government agencies under Article 68 of Law No. 8/2004 (see 'Disclosure of communications data' above).

In our view, these are wide enough that, in each case, they could be interpreted as requiring a telecommunications operator to decrypt communications data, where that operator has applied the encryption. This is because the operator must cooperate with the competent authorities to achieve these outcomes.

Another reason for this interpretation is that the general obligation of secrecy of communications contained in Article 68 of Law No. 8/2004 contains an exception in cases provided by law in criminal prosecutions matters or of interest to the national security and the prevention of terrorism, criminality and organised delinquency. Therefore, the fact that the concept of secrecy of communications is not absolute implies that decryption would be acceptable in one of the excepted circumstances.

Mozambique

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

No. The scenario is not addressed under Mozambican Law.

Our understanding of the existing law is that a telecommunications operator must cooperate with the competent authorities to provide real-time lawful interception assistance and disclose communications data (see Question 1 above). It is unclear how far such cooperation can go if the operator lacks the technological ability to decrypt a third party's encryption.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

No. The law currently in force doesn't regulate this matter and therefore does not expressly prohibit a telecommunications operator from offering end-to-end encryption on its communication services.

Nonetheless, we think that offering end-to-end encryption may be interpreted as incompatible with a telecommunication operator's obligation to cooperate with the competent authorities with regard to the legal interception and disclosure of communications data (see Question 1). We cannot be certain of this, as the law does not establish procedures for this cooperation, nor make clear the nature and extent of cooperation required from a telecommunications operator.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

No. Mozambique is governed by Roman-Germanic system any interference by the state and/or government should be based on the law. However if there's no legislation they can resort to custom, doctrine and jurisprudence.

The Netherlands

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016..

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

Telecommunications Act

According to Article 13.1 of the Telecommunications Act (the **TCA**), providers of public telecommunications networks and publicly available telecommunications services (service providers) will only make their telecommunications networks and services available to users if these can be wiretapped. Rules may be set by or follow a general administrative order regarding the technical susceptibility to tapping of public telecommunications networks and publicly available telecommunications services.

The TCA requires public telecommunications service providers to set up and maintain a reasonable interception capability in their networks. This includes being able to implement an interception after having received an interception warrant.

Note that the service provider will bear the costs of the investment, exploitation and maintenance of the interception capabilities.

In addition, failure to comply with an interception warrant is a criminal offence (Article 184 of the Dutch Criminal Code (*Wetboek van Strafrecht* or **DCC**).

Dutch Code of Criminal Procedure

Article 13.2 of the TCA obliges providers of public telecommunications networks to cooperate with the enforcement of an administrative order according to the Dutch Code of Criminal Procedure (*Wetboek van Strafvordering* or **DCCP**) or consent according to the Intelligence and Security Services Act 2002 (*Wet op de inlichtingen- en veiligheidsdiensten 2002* or **ISSA**) over the tapping or recording of communications that takes place via their telecommunications networks, or for the communications handled by them. Service providers are required to take all reasonable practical steps requested by the relevant authority to comply with an interception warrant.

It follows from Articles 126(m) (serious crime), 126(t) (planned organised crime) and 126(zg) (indications of terrorist crime) of the DCCP that a supervisory judge can issue an interception warrant where the public prosecutor believes it is necessary for the investigation of criminal cases.

The Minister of Interior and Kingdom Relations may, furthermore, authorise interception by the General Intelligence and Security Service (*Algemene Inlichtingen- en Veiligheidsdienst* or **AIVD**) and the Minister of Defence may authorise interception by the Military Intelligence and Security Service (*Militaire Inlichtingen- en Veiligheidsdienst* or **MIVD**) according to Article 25 of the ISSA. Interception by the MIVD outside military territory also requires the authorisation of the Minister of Interior Affairs.

It should be noted that illegal interception is a criminal offence (Article 139c of the DCC) which can lead to a penalty of maximum EUR82,000.

2. Disclosure of communications data

The TCA requires service providers to store traffic data. This data would include the location of the cell of origin.

Article 13.4 of the TCA states that the service provider is obliged to provide the data requested on the basis of Articles 126(n), 126(na), 126(u) and 126(ua) of the DCCP.

Moreover, the service provider is obliged to disclose data to the AIVD and MIVD on the basis of Article 28 of the ISSA. The ISSA also includes an obligation to cooperate in decrypting the data.

The service provider is obliged to retain and/or provide location data, traffic data and data which can identify the user of the telecommunications network (Article 13.2(a) of the TCA and Articles 126(ng), 126(ug) and 126(zh) of the DCCP. Generally, the content of customer communications is not stored. However, Articles 126(ng), 126(ud) and 126(ug) of the DCCP state that a provider can be obliged to provide stored data when it can reasonably be expected that it has access to such data. In addition, the service provider can be obliged to cooperate in the decryption of the data (Articles 126(nh) and 126(uh) of the DCCP).

Article 13.2(a) of the TCA states that the service provider is obliged to retain certain information. According to Article 13.2(b) of the TCA, the service provider is obliged to cooperate with an order on the basis of Articles 126(hh), 126(ii), 126(nc)–126(ni) and 126(uc)–126(ui) of the DCCP, and to disclose such information to the law enforcement agency.

The Netherlands

3. National security and emergency powers

In exceptional circumstances connected with the enforcement of international rules of law, international relations or war, the Minister of Economic Affairs may issue instructions, in agreement with the Minister of Foreign Affairs, to providers of public telecommunications networks and publicly available telecommunications services regarding the provision of telecommunications from and to other countries. In agreement with the Minister of Security and Justice, the Minister of Economic Affairs may also issue instructions to such providers regarding the use of messages from government bodies to warn the public of impending disasters or emergencies (Article 14.1 of the TCA).

In addition, under Article 14.4 of the TCA (which at the time of writing has not yet entered into force) and in the event of the necessary exceptional circumstances, the Minister of Economic Affairs will be able to give instructions to service providers concerning the maintenance and exploitation or use of their public telecommunications networks. In the case of a war, the Minister of Economic Affairs may only give such instructions in agreement with the Minister of Defence (Article 14.3 of the TCA). According to Article 14.2 of the TCA, Article 14.4 of the TCA may only enter into force in exceptional circumstances, by Royal Decree and on the recommendation of the Prime Minister.

4. Oversight of the use of powers

Instructions given by the Minister of Economic Affairs cannot be appealed and the authorisation of a supervisory judge must be obtained in respect of the investigations of criminal cases.

Censorship-related powers

1. Shut-down of network and services

Telecommunications Act

Under Article 14.4 of the Telecommunications Act (TCA), in exceptional circumstances (usually war, terrorism, natural disaster, etc), the Minister of Economic Affairs may require network providers such as Vodafone to maintain, market or use their telecommunications networks in line with his or her instructions. Although it is not explicitly stated in the TCA, the Minster might be able to instruct Vodafone to shut down its entire network or a particular service.

2. Blocking of URLs and IP addresses

Telecommunications Act

As set out above, Article 14.4 of the TCA gives the Minister of Economic Affairs wide powers in exceptional circumstances. Although it is not explicitly stated in the TCA, it cannot be excluded that the Minster might instruct Vodafone to block URLs or IP addresses.

3. Power to take control of Vodafone's network

As set out above, Article 14.4 of the TCA gives the Minister of Economic Affairs wide powers in exceptional circumstances. Although it is not explicitly stated in the TCA, the nature of the powers given to the Minister could effectively extend to taking control of Vodafone's network.

4. Oversight of the use of powers

Telecommunications Act

Instructions given by the Minister of Economic Affairs under Article 14.4 of the TCA cannot be appealed.

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes. Article 13.2 of the TCA contains an obligation to cooperate with decrypting (with reference to Articles 126m (severe infringement of the legal order) and 126t of the DCCP).

Article 13.2b of the TCA also contains an obligation to cooperate with decryption (with reference to Articles 126nh (fairly serious crime), 126uh (planned serious organised crime) and126zp (indications of terrorist crime) of the DCCP. Moreover, Article 2(e) of the Decision of Interception of Public Communication Networks and Services (*Besluit aftappen openbare communicatienetwerken en -diensten,* **DIPC**) contains an obligation to disclose data without cryptography.

The Netherlands

According to Article 25 of the ISSA, anyone who knows how to remove the encryption of conversations, telecommunications or data transfer is obliged to provide all necessary cooperation in order to decrypt such communications.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

According to Article 13.2 of the TCA (with reference to Articles 126m and 126t of the DCCP) and Article 13.2b of the TCA (with reference to Articles 126nh, 126uh and 126zp of the DCCP), a provider may be ordered to cooperate in the decryption or to make its knowledge of the encryption available, if there are good grounds to suspect that it has knowledge of the way the data is encrypted. According to Article 25 of the ISS, 'anyone' who has knowledge of the way of removing the encryption of conversations, telecommunications or data transfer, is obliged to provide all necessary cooperation in order to decrypt such communications.

Given this broad wording, it may be that if telecommunications operators are able to provide equipment interference or if it is technically possible for them to interfere with the set-up of encryption and the subsequent communications in such a way that they gain access to the cleartext data, they could be ordered to decrypt the data.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

No. According to Article 13.1 of the TCA, providers of public telecommunications networks and publicly available telecommunications services will only make their telecommunications networks and services available to users if these can be wiretapped.

According to Articles 13.2 and 13.2b of the TCA, Article 25 of the ISS and Article 2(e) of the DIPC, a service provider has to disclose data without the encryption it has applied, or must cooperate with the decryption or make its knowledge regarding the encryption available, if there are good grounds to suspect that it has knowledge of the way in which data is encrypted.

If the software provided by a telecommunications operator enables customers themselves to encrypt their communications and the telecommunications operator is not able to decrypt the data or has no knowledge of the way in which the data is encrypted, we take the view that a telecommunications operator could face a challenge under Article 13.1 of the TCA.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

In our research, we have not found any examples of the Dutch government using legislation, other than the legislation mentioned above, to demand access to data protected by encryption.

New Zealand

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

On 11 May 2014 the Telecommunications (Interception Capability) Act 2004 (**TICA**) was repealed and fully replaced by the Telecommunications (Interception Capability and Security) Act 2013 (**TICSA**). The TICSA contains much of the same requirements set out in the TICA, and goes further in introducing new obligations. For completeness, we also note that under the TICSA, network operators are now required to register certain details, such as their contact details and details of their general operations, on the register of network operators set up by the Commissioner of Police.

The New Zealand Telecommunications Carriers Forum (TCF) has, in consultation with the main telecommunications carriers and surveillance agencies in New Zealand, produced the Guidelines for Interception Capability (the Guidelines) for compliance with the New Zealand telecommunications interception capability laws. The Guidelines make reference to the European Telecommunications Standards Institute standards. The Guidelines and the standards they prescribe are voluntary obligations, and are not legal requirements. The Guidelines (as at April 2016) are based on the now repealed TICA. Accordingly, the Guidelines (as updated from time to time) may be replaced or removed under the new TICSA. The Guidelines should prove useful in indicating the best practice approach that should be adopted by network operators to comply with some of New Zealand's interception capability requirements.

1. Provision of real-time lawful interception assistance

The information outlined below represents the law as in effect at April 2016. On 11 May 2014 the TICA was repealed and fully replaced by the TICSA. The TICSA contains much of the same requirements set out in the TICA, and goes further in introducing new obligations. For completeness, note that under the TICSA, network operators are now required to register certain details, such as their contact details and details of their general operations, on the register of network operators set up by the Commissioner of Police.

The Telecommunications (Interception Capability and Security) Act 2013 (TICSA)

The TICSA is New Zealand's primary piece of legislation governing the interception of telecommunications. The TICSA requires a network operator to assist a surveillance agency in the interception of telecommunications upon receipt of an interception warrant or evidence of other lawful interception authority (for the purposes of this report, these two forms of interception authority will together be referred to as interception warrants and only distinguished when necessary).

The government has the legal authority to issue an interception warrant, giving rise to an obligation for a network operator to assist in the interception of telecommunications under the TICSA, under the following enactments:

- the Government Communications Security Bureau Act 2003 (the GCSB Act);
- the Search and Surveillance Act 2012 (SAS Act); and
- the New Zealand Security Intelligence Service Act 1969 (the NZSIS Act).

Section 24 of the TICSA requires a network operator who is shown a copy of an interception warrant authority to assist a surveillance agency in the interception of individual customer communications by:

- making available any officers, employees or agents who are able to provide any reasonable technical assistance that may be necessary for the agency to intercept a telecommunication that is subject to the interception warrant; and
- taking all other reasonable steps that are necessary for the purpose of giving effect to the interception warrant, including, among other things, assisting to:
  - identify and intercept telecommunications without intercepting telecommunications that are not authorised to be intercepted;
  - carry out the interception of telecommunications unobtrusively, without unduly interfering with any telecommunications, and in a manner that protects the privacy of telecommunications that are not authorised to be intercepted; and
  - undertake the actions efficiently and effectively, and:
    - if it is reasonably achievable, at the time of transmission of the telecommunication; or
    - if it is not reasonably achievable, as close as practicable to that time.

New Zealand

In addition, Section 9 of the TICSA requires network operators with more than 4,000 customers to ensure that every public telecommunications network that the operator owns, controls or operates and every telecommunications service that the operator provides in New Zealand has an interception capability. An interception capability includes the duty to ensure that the interception capability is developed, installed and maintained (see Section 9(3) of the TICSA).

Under Section 10(1) of the TICSA, a network operator will have complied with this interception capability obligation if every surveillance agency that is authorised by an interception warrant is able to:

- identify and intercept telecommunications without intercepting telecommunications that are not authorised to be intercepted;
- obtain call-associated data relating to telecommunications (other than telecommunications that are not authorised to be intercepted);
- obtain call-associated data and the content of telecommunications (other than telecommunications that are not authorised to be intercepted) in a usable format;
- carry out the interception of telecommunications unobtrusively, without unduly interfering with any telecommunications, and in a manner that protects the privacy of telecommunications that are not authorised to be intercepted; and
- undertake these actions efficiently and effectively at the time of transmission of the telecommunication or, if it is not reasonably achievable to do so, as close as practicable to that time.

Notably, under Sections 14 and 15 of the TICSA, a network operator does not have to provide an interception capability in respect to:

- any infrastructure-level service it provides (ie the provision of a physical medium, such as optical fibre cable, over which telecommunications are transmitted); or
- any wholesale network service it provides (ie a service provided by a network operator to another network operator over a network it owns and operates). Although, the network operator must still ensure that the wholesale network service is 'intercept accessible', as that phrase is defined under Section 12 of the TICSA.

However, the Minister for Communications and Information Technology, on application by a surveillance agency (see Section 17 of the TICSA), reserves the right to make a direction requiring a network operator providing an infrastructure-level service or a wholesale network service to:

- provide full interception capabilities in respect to the service in the manner described under Section 10(1) of the TICSA; or
- ensure that the service is 'intercept accessible' or 'intercept ready' (as those terms are defined in Sections 11 and 12 of the TICSA).

Network operators providing these infrastructure-level or wholesale network services are typically subject to less strenuous requirements under the TICSA, only being required to be intercept ready or intercept accessible as opposed to having full interception capability. Similarly, under Section 20 of the TICSA, the Governor-General of New Zealand may, by Order in Council, on the recommendation of the Minister for Communications and Information Technology, make regulations requiring particular network operators, regardless of the service they operate, to comply with Section 9 of the TICSA and thus ensure that their services have full interception capability.

Section 24 of the TICSA also requires a network operator who is shown a copy of an interception warrant to assist a surveillance agency by making available any officers, employees or agents who are able to provide any reasonable technical assistance that may be necessary for the agency to intercept a telecommunication that is subject to the warrant or authority. Therefore, under the TICSA, on receipt of an interception warrant a network operator could be required to assist in the implementation of interception capabilities on the network operator's network.

Section 26 of the TICSA requires that, while assisting in the interception of a telecommunication, a network operator must take all practicable steps that are reasonable in the circumstances to minimise the likelihood of intercepting telecommunications that are not authorised to be intercepted.

Under Section 114 of the TICSA, the cost of implementing the interception capability must be borne by the network operator. Subject to limited circumstances, the surveillance agency presenting the interception warrant is responsible for paying the actual and reasonable costs incurred by a network operator in assisting the agency (see Section 115 of the TICSA).

An interception warrant requiring a network operator to assist in the interception of individual customer communications under the TICSA could be issued under the following enactments in the described circumstances:

New Zealand

Government Communications Security Bureau Act 2003 (GCSB Act)

Under Section 15A(1)(a) of the GCSB Act, the Director (defined as being the chief executive of the Government Communications Security Bureau (the GCSB)) can apply to the Minister responsible for the GCSB (the GCSB Minister) for an interception warrant authorising the use of interception devices to intercept particular kinds of communications. The GCSB Minister can grant the interception warrant if, among other things, the GCSB Minister is satisfied that that the proposed interception is for the purpose of cybersecurity and intelligence gathering. The interception warrant may request a person to give assistance that is reasonably necessary to give effect to the warrant (see Section 15E of the GCSB Act). Therefore, an interception warrant issued under the GCSB Act may require a network operator to assist in the interception of telecommunications through the installation of interception devices on its own network, in compliance with its obligations under Section 24 of the TICSA.

Section 24 of the GCSB Act imposes a duty on those assisting in an interception to minimise the likelihood of intercepting communications that are not relevant to the persons whose communications are to be intercepted.

Search and Surveillance Act 2012 (SAS Act)

Under Section 53 of the SAS Act, a District Court Judge or a Judge of the High Court (a Judge) may issue a surveillance device warrant (a form of interception warrant under the TICSA) on application by an enforcement officer (in most cases, a constable). A Judge may grant a surveillance device warrant if the Judge is satisfied that there are reasonable grounds to suspect that an offence has been, or will be, committed and that the proposed use of the surveillance device will obtain information that is evidential material in respect of the offence. A surveillance device warrant permits, among other things, an enforcement officer to use an interception device to intercept a private communication and may specify that the enforcement officer use any assistance that is reasonable in the circumstances (see Section 55(3)(f)). Therefore, an interception warrant issued under the SAS Act may require a network operator to assist in the interception of telecommunications through the installation of an interception device on its own network, in compliance with its obligations under Section 24 of the TICSA.

The New Zealand Security Intelligence Service Act 1969 (NZSIS Act)

Under Section 4A(1) of the NZSIS Act, the Minister in charge of the New Zealand Security Intelligence Service (NZSIS) (the NZSIS Minister) and the Commissioner of Security Warrants may jointly issue a domestic intelligence warrant, or, under Section 4A(2) of the NZSIS Act, the NZSIS Minister acting alone may issue a foreign intelligence warrant (both intelligence warrants being a form of interception warrant under the TICSA). An intelligence warrant may be issued if the interception to be authorised is necessary for, among other things, the detection of activities prejudicial to security, or for the purpose of gathering foreign intelligence information essential to security. An intelligence warrant authorises a person to, among other things, intercept or seize any communication, document or item not otherwise lawfully obtainable by the person, including the installation or modification of any device or equipment. The Director of Security may request any person or organisation to give specified assistance to an authorised person for the purpose of giving effect to an intelligence warrant. Therefore, an intelligence warrant issued under the NZSIS Act may require a network operator to assist in the interception of telecommunications, in compliance with its obligations under Section 24 of the TICSA.

2. Disclosure of communications data

The Telecommunications (Interception Capability and Security) Act 2013 (TICSA)

Section 24 of the TICSA requires a network operator who is shown a copy of an interception warrant to assist a surveillance agency by, among other things, assisting in obtaining call associated data and the stored content relating to telecommunications.

Call-associated data includes data that is generated as a result of the making of the telecommunication (whether or not the telecommunication is sent or received successfully) and that identifies the origin, direction, destination or termination of the telecommunication, as well as more specific information (see Section 3 of the TICSA). If the metadata relating to customer communications being requested by the government under an interception warrant falls within the definition of call-associated data, a network operator would be required to assist the surveillance agency in obtaining that data.

The surveillance agency with the interception warrant is responsible for paying the actual and reasonable costs incurred by a network operator in assisting the agency.

New Zealand

An interception warrant requiring a network operator to assist in the obtaining of call-associated data or stored content could be issued under the following enactments in the described circumstances:

- **The GSCB Act**
  In relation to Section 15A(1)(a) of the GCSB Act, in particular circumstances the GCSB Minister may, under Section 15A(1)(b) of the GCSB Act, grant an access authorisation (a form of interception warrant) authorising access to the information infrastructure of a network operator, which includes all communications and information contained within its communications systems and networks. The access authorisation may request a person to give assistance that is reasonably necessary to give effect to the authorisation (see Section 15E of the GCSB Act). Therefore, an access authorisation issued under the GCSB Act may require a network operator to assist a surveillance agency by granting access to its communications contained in its information infrastructure, and hence any metadata (being information that would constitute a 'communication') and any stored communications that the network operator holds.
- **The SAS Act**
  A surveillance warrant could require a network operator to disclose metadata relating to customer communications to aid the enforcement officer in its interception efforts. Similarly, and in any event, a surveillance device warrant allows an enforcement officer to require a network operator to disclose call-associated data in relation to a telecommunication of which the content has already been intercepted by the enforcement officer (see Section 55(3)(g) of the SAS Act) (ie if the content of the telecommunications has already been obtained by the enforcement officer through another means).
- **The NZSIS Act**
  As a document includes any information stored by any means (see definition under Section 2(1) of the Official Information Act 1982), an interception warrant issued under the NZSIS Act could require the disclosure of all metadata information that a network operator holds, as well as the stored content of telecommunications. A network operator would then, in being required to assist in the execution of a warrant, be required to obtain call-associated data and communications content under Section 24(b)(iii) of the TICSA (if the metadata requested under the SAS Act was not already held).

In addition, under Sections 71 and 74 of the SAS Act, an enforcement officer may apply to an issuing officer for a production order against a person in respect of documents. Documents are defined as including call-associated data (which could include metadata) and the content of telecommunications in respect of which, at the time an application is made for a production order against a network operator, the network operator has storage capability for, and stores in the normal course of its business, that data and content.

A production order will only be made if:

- there are reasonable grounds to suspect that a specified offence has been, or will be, committed;
- the documents sought by the proposed order are likely to constitute evidential material in respect of the offence; and
- the documents sought by the proposed order are in the possession or under the control of the person against whom the order is sought, or will come into his or her possession, or under his or her control while the order is in force (see Section 72).

When the documents are produced under a production order, the enforcement officer may retain the original copies, or take copies, or require the person producing the documents to reproduce the information recorded in the documents in a usable form (see Section 78 of the SAS Act). An original copy must be returned as soon as possible (see Section 79 of the SAS Act).

Harmful Digital Communications Act 2015 (HDC Act)

Under the HDC Act, the District Court can order that an online content host, among other things, takes down or disables public access to particular material that has been posted or sent and order that the identity of the author of an anonymous or pseudonymous communication be released to the court.

3. National security and emergency powers

The government's power to issue intelligence warrants (a form of interception warrant under the TICSA) on the grounds of national security under Section 4A of the NZSIS Act, and the possible assistance the intelligence warrants can require from network operators, is outlined above.

New Zealand

International Terrorism (Emergency Powers) Act 1987 (ITEPA)

Under Section 10 of the ITEPA, in the circumstances of an international terrorist emergency where emergency powers are exercisable, a constable may requisition any land, building or equipment within the area in which the emergency is occurring and place the property under the control of a constable. This could conceivably involve the requisitioning of a network operator's network equipment.

Further, under the ITEPA, a constable may, for the purpose of preserving life threatened by any emergency:

- connect any additional apparatus to, or otherwise interfere with the operation of, any part of the telecommunications system; and
- intercept private communications.

This power specified may be exercised only by, or with the authority of, a constable who is of or above the level of position of inspector, and only if that constable believes, on reasonable grounds, that the exercise of that power will facilitate the preservation of life threatened by the emergency. This power would again constitute a 'lawful interception authority' under the TICSA (being an authority to intercept communications in an emergency situation granted to a member of a surveillance agency), thus imposing obligations on network operators to assist the enforcement officer under the TICSA just as they would be required to when shown an interception warrant.

Under Section 18 of the ITEPA, no person who intercepts or assists in the interception of a private communication (such as a network operator) under Section 10(3), or acquires knowledge of a private communication as a direct or indirect result of that interception, shall knowingly disclose the substance, meaning or purport of that communication, or any part of that communication, otherwise than in the performance of that person's duty.

4. Oversight of the use of powers

Under Section 15 of the GCSB Act, the GCSB Minister authorises a warrant if, among other things, the Minister is satisfied that the proposed interception is for the purpose of cybersecurity and intelligence gathering.

Under Section 53 of the SAS Act, only a Judge may issue a surveillance device warrant. Further, only a Judge or a person such as a Justice of the Peace, Community Magistrate, Registrar or Deputy Registrar, who is for the time being authorised to, may act as an issuing officer under Section 108 of the SAS Act and make a production order.

Under Sections 158 and 159 of the SAS Act, a person who has an interest in the produced documents (ie a customer of a network operator) may apply to the District Court for access to, or the release of, the things produced.

Under Section 4A(5) of the NZSIS Act, when the identification of foreign capabilities that impact on New Zealand's international or economic wellbeing is in issue, before issuing an intelligence warrant the NZSIS Minister must consult with the Minister of Foreign Affairs and Trade about the proposed intelligence warrant.

Censorship-related powers

1. Shut-down of network and services

The government does not have the legal authority to order the shut-down of Vodafone's network or services.

International Terrorism (Emergency Powers) Act 1987 (ITEPA)

Under Section 10 of the ITEPA, in the circumstances of an international terrorist emergency, a police constable may requisition any property (including land, buildings and equipment) of a network operator within the area in which the emergency is occurring. While it is conceivably possible that the practical effect of seizing certain equipment may mean that the relevant network operator's network (such as Vodafone's) is shut down, the Act does not give the government a legal right to shut down the network.

2. Blocking of URLs and IP addresses

Films, Videos, and Publications Classification Act 1993

Under the Films, Videos, and Publications Classification Act 1993, viewing or owning certain types of material (for example, depictions of bestiality or child sex abuse) is forbidden; this applies to material accessed over the internet.

While there is no legal authority for the government to block a URL or IP address, the New Zealand Department of Internal Affairs operates the Digital Child Exploitation Filtering System (DCEFS) in partnership with a number of New Zealand internet service providers, including Vodafone. Participation in DCEFS is voluntary.

Under the DCEFS, the Department of Internal Affairs maintains a list of banned websites and their URLs. Using a routine protocol it has in place with the participating internet service providers, each time a person tries to access a website (banned or not), their request is routed through the Department of Internal Affairs' server; that server filters each request to determine whether access to the website is allowed. If the website URL is on the list of banned websites, access to it is refused.

New Zealand

3. Power to take control of Vodafone's network

The government does not have the legal authority to take control of Vodafone's network.

International Terrorism (Emergency Powers) Act 1987 (ITEPA)

Please see Section 1 'Shut-down of network and services' above. While it is conceivable that the practical effect of the government's use of its powers under the ITEPA could be used to the extent that the government effectively took control of a network provider's network, the Act does not provide the government with explicit authority to do this.

4. Oversight of the use of powers

International Terrorism (Emergency Powers) Act 1987 (ITEPA)

Sections 5 to 8 govern police authority to use the emergency powers provided for under Section 10. Under Section 5, the police commissioner must inform the prime minister as soon as he or she believes that an emergency is occurring; the emergency may be an international terrorist emergency; and the exercise of emergency powers is or may be necessary to deal with that emergency.

Upon being so informed, the prime minister may then hold a meeting with a minimum of three Ministers of the Crown to consider whether to authorise use of the emergency powers. If the Ministers of the Crown present at the meeting believe on reasonable grounds that an emergency is occurring, that may be an international terrorist emergency and the exercise of emergency powers is necessary to deal with the emergency, the Minister of the Crown presiding at the meeting may give notice in writing authorising the exercise of emergency powers by the police. Upon authorisation the Minister of the Crown who presided must inform the House of Representatives that the authorisation has been given and the reasons why it was given. The House of Representatives may resolve to, from time to time, extend that authorisation for no longer than seven days pursuant to Section 7. The House of Representatives may also, at any time, revoke the authorisation pursuant to Section 8. Section 6 requires the Minister who signs the notice authorising the use of emergency powers to inform the public by such means as are reasonable in the circumstances and to publish the authorised notice in the Gazette as soon as practicable.

The authority to exercise the emergency powers expires once the police commissioner is satisfied that the emergency has ended, or is deemed not to be an international terrorist emergency, or at the close of seven days after the day on which the notice under Section 5 was given, whichever is sooner.

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes. The TICSA requires a network operator who is shown a copy of an interception warrant to decrypt a telecommunication on its own public telecommunications network or service if it has provided the encryption.

Sections 10(3) and 24(4) of the TICSA require a network operator to, for the purpose of obtaining data in a usable format and in giving effect to an interception warrant, assist in decrypting a telecommunication on its own public telecommunications network or telecommunications service if it has provided the encryption for that telecommunication.

An interception warrant requiring a network operator to assist in decrypting a telecommunication it has encrypted could be issued as an access authorisation under the GSCB Act; a surveillance warrant under the SAS Act; and/or an intelligence warrant under the NZSIS Act (see earlier in this chapter under 'Provision of real-time lawful interception assistance' for a more detailed explanation of each of these types of warrant).

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

No. Under Sections 10(4) and 24(4) of the TICSA, a network operator is not required to decrypt a telecommunication on its own telecommunications network or service if the encryption has been provided by means of a product supplied by a person other than the network operator and is available on retail sale to the public or is supplied by the network operator as an agent for that product.

The default position under Sections 10(3) and 24(3)(vi) of the TICSA requires a network operator to, for the purpose of obtaining data in a usable format and/or in giving effect to an interception warrant, assist in decrypting a telecommunication on its own public telecommunications network or telecommunications service if it has provided the encryption for that telecommunication.

Furthermore, under Sections 10(4) and 24(4) of the TICSA, a network operator is not required to decrypt any such telecommunication if the encryption has been provided by means of a product that is supplied by a person other than the network operator and is available to the public or is supplied by the network operator as an agent for that product.

New Zealand

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

No, although the answer here is not legally certain.

The TICSA requires a network operator to, in certain circumstances, assist in decrypting a telecommunication on its own public telecommunications network or telecommunications service if it has provided the encryption for that telecommunication.

The default position under Sections 10(3) and 24(3)(vi) of the TICSA requires a network operator to, for the purpose of obtaining data in a usable format and/or in giving effect to an interception warrant, assist in decrypting a telecommunication on its own public telecommunications network or telecommunications service if it has provided the encryption for that telecommunication.

Under Sections 10(4) and 24(4) of the TICSA, a network operator is not required to decrypt any such telecommunication if the encryption has been provided by means of a product that is supplied by a person other than the network operator and is available to the public or is supplied by the network operator as an agent for that product.

It can be inferred from this that if the encryption has been provided by means of a product that is supplied by the network operator (not acting as an agent), then the network operator would be required to decrypt the telecommunication. However, no guidance or opinion has been issued by the telecommunications regulation in New Zealand on this subject.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

We have not found any examples where this has occurred in New Zealand.

Portugal

In this report, we provide an overview of some of the legal powers under the law of Portugal that Portuguese courts have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as network censorship, content blocking and restrictions on freedom of expression. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

The Constitution of the Portuguese Republic

There are two instances in which the courts can authorise and demand the provision of real-time interception assistance:

1. According to Article 34,4 of the Constitution of the Portuguese Republic, interception of telephone communications is only expressly allowed in the context of criminal investigations which are not the responsibility of the government but of the Public Prosecutor jointly with a criminal judge; and
2. Articles 19, 134 and 138 of the Constitution, as well as Law No. 44/86 30 September (Legal Framework for the State of Siege and Emergency), permit the suspension of certain rights, liberties and guarantees by national bodies of sovereignty (including the government) in the event that a state of siege or emergency has been decreed by the President of the Republic and approved by the Portuguese Parliament. The states of siege or emergency decree shall expressly determine which rights, liberties and guarantees shall be suspended. In theory, this legal framework could enable the government to demand that a communications service provider assist in intercepting customer communications provided that it has been foreseen in the states of siege or emergency decree that the fundamental rights of Article 34 of the Constitution are suspended. Nevertheless, the government order should be communicated to a judge afterwards for validation.

Should interception of communications be carried out in any other context, this would be considered illegal, a breach of the Constitution and punishable as a crime.

Portuguese Criminal Proceedings Code

For the interception of communications in the context of a criminal proceeding, following the rules established in Articles 187–190 of the Portuguese Criminal Proceedings Code, interception may only be authorised in cases of suspicion of crime and after criminal proceedings are opened.

The interception may only be authorised by a judge if the crime under investigation is, for example, one of the following:

i. crimes punished with imprisonment which maximum limit is not less than three years;
ii. narcotraffic;
iii. possession of prohibited weapons and weapon trafficking;
iv. contraband;
v. crimes which consist of offending, threatening and disturbing privacy and carried out by telephone;
vi. terrorism; or
vii. organised crime

To perform communications interceptions an authorisation from a judge is always required. Only the Public Prosecutor (who is in charge of the investigation) may decide to request authorisation from the judge for the interception.

Law No. 9/2007 of 19 February, which sets out the legal framework for the Portuguese Information Security System (*Sistema de Informações*/SIS) and for the Portuguese Services for Strategic Defence (SIED), and also sets out the purposes and attributions of the bodies responsible for managing information, security and national strategic defence in Portugal, does not grant powers of interception, encryption/decryption, direct access to communications or the possibility of requesting such access being granted by electronic communications service providers. Such access is only possible under the terms of the Portuguese Criminal Proceedings Code, in the context of a judicial procedure, as set out above.

Law No. 53/2008

Law No. 53/2008 of 29 August, establishes the legal provisions applicable to homeland security in Portugal. This law states that access and control of communications may only be carried out following a judicial authorisation and performed solely by the police.

Portuguese Electronic Communications Law

Under Article 27/o' of the Portuguese Electronic Communications Law (Law 5/2004 of 10 February) and the operating licences granted to communications service providers, on the providers of electronic communications

Portugal

services and networks must provide, at their own expense, systems for legal interception by competent national authorities, as well as the means for decryption or decoding where these facilities are present.

2. Disclosure of communications data

Under Portuguese law, only ICP-ANACOM (National Regulatory Authority for the electronic communications sector) or Comissão Nacional de Protecção de Dados (National Data Protection Authority) can access or order the disclosure of metadata, and only within the scope of their powers to supervise, monitor and investigate (particularly in the case of a customer complaint) compliance with the laws and regulations applicable to the electronic communications sector and in respect of compliance with data protection and privacy laws.

ICP-ANACOM's legal powers are defined in Law No. 5/2004 of 10 February (electronic communications law) and in Decree-Law No. 309/2001 of 7 December (ANACOM Statute). Comissão Nacional de Protecção de Dados legal powers are defined in Law No. 67/98 of 26 October (Portuguese Data Protection Act) and Law No. 43/2004 of 18 August (organic law for the National Data Protection Authority).

Apart from these authorities, no other government department or law enforcement agency can order the disclosure of metadata. Such information can only be obtained under the rules set out above for provision of real-time lawful interception assistance, namely in the context of a criminal proceeding, and provided that a judicial authorisation has been sought and the rules established in Articles 189–190 of the Portuguese Criminal Proceedings Code are followed. However, if a state of siege or emergency has been decreed, the exceptional rules set out above may also apply.

3. National security and emergency powers

The Portuguese National security agency is exclusively competent to gather intelligence to prevent threats to national security. Therefore, under the Law No. 30/84 of 5 September, the agency is not allowed to pursue actions that may constitute an offence to the fundamental rights, liberties and guarantees set out in the Portuguese Constitution and Law.

Additionally, this law establishes that the agency does not have powers to pursue any acts that are within the scope of the courts, and police authorities' competence.

If it is suspected that a crime is being committed against national security, the Portuguese National security agency must inform the Public Prosecutor so that a criminal proceeding can be opened and, if relevant to the investigation, the Public Prosecutor may request to a judge the gathering of evidence (eg through real-time interception or disclosure of metadata) according to the regime described above.

Constitution of the Portuguese Republic

Articles 19, 134 and 138 of the Constitution of the Portuguese Republic, as well as Law No. 44/86, dated 30 September (Legal Framework for the State of Siege or State of Emergency) permits the suspension of certain rights, liberties and guarantees in the event that a state of siege or emergency has been decreed by the President of the Republic, after consulting the government, and approved by the Portuguese Parliament. The state of siege or emergency decree shall expressly determine which rights, liberties and guarantees shall be suspended.

The state of siege or emergency decree would only be effective upon specific enforcement by the President. These powers are exceptional and may only last for a maximum of 15 days (or if otherwise decided by law). These states of siege or emergency may only be determined if absolutely necessary, in the event of an effective or imminent aggression by foreign forces, grave threat or disturbance of the normal, democratic constitutional order, or public calamity. Any powers granted to the government in this respect will apply in very limited circumstances and only to the extent required and adequate for the purpose at hand.

4. Oversight of the use of powers

The provision of oversight in respect of the powers of interception and disclosure of communications data are set out in the sections above.

Censorship-related powers

1. Shut-down of network and services

Constitution of the Portuguese Republic and Law No. 44/86 of 30 September

The Portuguese government may order the shut-down of providers' networks and services (including Vodafone's) should a 'state of siege or emergency' be declared.

A state of siege or emergency is declared by the President of the Portuguese Republic and it depends on the hearing of the government and parliamentary approval. It is exceptional and is only declared when absolutely necessary in the event of a serious threat or disturbance to Portugal's normal, democratic

Portugal

constitutional order, such as a public calamity or imminent aggression by foreign forces. It may last up to a maximum of 15 days, subject to possible renewal for one or more similar terms if the situation that gave rise to the declaration of state of siege or emergency persists.

Articles 19, 134 and 138 of the Constitution of the Portuguese Republic and Law No. 44/86 of 30 September (Legal Framework for the State of Siege and Emergency) allow the suspension of rights, liberties and guarantees by sovereign national bodies (including the Portuguese government) in the event that a state of siege or emergency is decreed. This power is wide-ranging and therefore could allow the government to shut down Vodafone's network or services.

Electronic Communications Law (Law No. 5/2004 of 10 February)

Under Articles 110 and 111 of the Electronic Communications Law, the Portuguese national authority for telecommunications (ANACOM) is empowered to take certain measures where a telecommunications provider (such as Vodafone) is in breach of its legal obligations under the Electronic Communications Law and the breach in question represents a serious and immediate threat to public security or health, or raises serious economic or operational problems for other electronic communications providers or network users.

In case of severe or repeated breaches of these obligations, where interim measures are unlikely to be sufficient, ANACOM may suspend an electronic communications provider's activities for up to two years or entirely revoke the provider's authorisation to provide network services. Therefore, ANACOM could suspend or revoke Vodafone's ability to provide its network and services (effectively shutting them down) if Vodafone were found to have committed a serious breach, or be repeatedly breaching, its obligations.

2. Blocking of URLs and IP addresses

Decree-Law No. 7/2004 of 7 January

According to Decree-Law 7/2004 of 7 January (Portuguese Electronic Commerce Law) only specific 'competent authorities' may order the blocking of IP addresses and/or ranges of IP addresses. These measures can be taken in case there is a serious threat to public health; public safety, particularly national safety and defence; consumers, including investors; and human dignity or public order, and include the protection of minors and repression of hatred incitement on grounds of race, sex, religion or nationality, especially for reasons of prevention or prosecution of crimes or misdemeanours. The measures undertaken must, of course, be proportionate. The competent authorities empowered to make such orders include the judicial courts, the National Regulatory Authority and, in certain circumstances, the National Authority for Cultural Activities (Inspeção Geral das Atividades Culturais).

3. Power to take control of Vodafone's network

Constitution of the Portuguese Republic and Law No. 44/86 of 30 September

See 'Shut-down of network and services' above. The government powers under a state of siege or emergency would extend to enabling the government to take control of Vodafone's network, should it choose to do so.

4. Oversight of the use of powers

Constitution of the Portuguese Republic and Law No. 44/86 of 30 September

Any powers granted to the Portuguese government in a state of siege or emergency are subject to the terms of the authorisation set by Parliament and must be proportionate. In addition, the declaration of state of siege or emergency does not preclude an individual's right of access to Portugal's courts under general law.

Electronic Communications Law (Law No. 5/2004 of 10 February)

The National Regulatory Authority must exercise its powers in an impartial, transparent and timely manner. Also, the measures undertaken by the National Regulatory Authority must be proportionate and reasonable. Decisions, orders or other measures adopted by the National Regulatory Authority are subject to judicial appeal.

Decree-Law No. 7/2004 of 7 January

Measures undertaken pursuant to the Electronic Commerce Law can be judicially challenged.

Portugal

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

No. The authority to require the telecommunications operator to intercept individual customer communications (and consequently unlock such data) lies only with a judge in the context of a criminal proceeding.

Note that the possible allocation of powers to the government in this context was discussed by the Portuguese Constitutional Court, and addressed in the Constitutional Court Judgment No. 403/2015. This discussion decided on the compliance of a proposed bill with the Portuguese Constitution. The purpose of the bill was to grant the Portuguese Information Security System (Sistema de Informações/SIS) and the Portuguese Services for Strategic Defence (SIED) the right to directly access traffic data and connected data regarding individuals' communications (along with other information). The Constitutional Court decided that the creation of any such right, in this context and on the terms proposed, did not comply with constitutional principles, including Article 34.4 of the Constitution.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

No. There is a specific framework for decryption obligations under Article 27(o) of the Electronic Communications Act whereby electronic communications service providers may be required to ensure the installation, at the undertaking's own expense, and provision of systems of legal interception to competent national authorities – Public Prosecutor and the courts (see 'Provision of real-time lawful interception assistance' above) – as well as the supply of means of decryption or decoding where these facilities are present, in accordance with legislation governing personal data and privacy protection within the scope of electronic communications. Note that in referring to the decryption framework in the Electronic Communications Act, the law does not state that the decryption obligation applies to *any* encrypted communication transmitted through the provider's network (ie including those communications that are encrypted by a third party).

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and content of the communication on receipt of a lawful demand?

The answer to this question will depend on the circumstances of the particular service in hand – this is a grey area of the law and there are a number of possible legal interpretations. For example, the answer to this question may vary depending on whether the telecommunications operator is offering a 'business as usual' telecommunications service (where the communication routes over the network as a data packet) or an 'over the top' communications service (where the delivery of a communication is made via Internet Protocol (IP) over the network) because such services may not be subject to the same type of decryption obligations. We are not aware of this topic having been expressly raised by a regulator to date in Portugal.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate as circa 1990) has been applied to contemporary cases involving encryption.

We are not aware of any examples where the government has applied legislation predating the advent of commercial encryption to this effect in Portugal.

Qatar

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

Decree Law No. (34) of 2006

Decree Law No. (34) of 2006 on the promulgation of the Telecommunications Law (the **Telecommunications Law**) and No. (1) of 2009 on the promulgation of the Executive By-Laws for the Telecommunications Law (the **Telecoms By-Laws**) require telecommunications systems operators that provide services to the public to intercept communications in real time.

Article 59 of the Telecommunications Law states that 'service providers must comply with the requirements of the security authorities in the state which relate to the dictates of maintaining national security and the directions of the governmental bodies in general emergency cases and must implement orders and instructions issued by the General Secretariat regarding the development of network or service functionality to meet such requirements.'

Any government department involved in state security can rely on Article 59 of the Telecommunications Law, together with the use of any enforcement powers vested directly in the concerned government authority.

Article 93 of the Telecoms By-Laws states that 'nothing in the By-Law prohibits or infringes upon the rights of authorised governmental authorities to access confidential information or communication relating to a customer, in accordance with the applicable laws.'

Article 91 of the Telecoms By-Laws mentions that service providers shall not intercept, monitor or alter the content of a customer communication, except with the customer's explicit consent or as expressly permitted or required by the applicable laws of the State of Qatar.

Article 4 of the Telecoms By-Laws authorises the Secretary General of the Ministry of Information and Communications Technology (ictQATAR) to issue regulations, decisions, rules, orders, instructions and notices for the implementation of the Telecommunications Law and the Telecoms By-Laws.

In cases involving national security and general emergency, the Qatari ministries and law enforcement agencies can directly approach communication service providers and require them to assist law enforcement agencies in achieving their objectives, which could involve implementing a technical capability that enables direct access to their network (without the communications service provider's operational control or oversight).

2. Disclosure of communications data

The powers outlined above in relation to real-time interception may also be used to order the disclosure of communications data.

3. National security and emergency powers

In all cases of national security and general emergency, the Qatari government agencies and law enforcement agencies can directly approach communications service providers to access their customers' communications data and/or network.

4. Oversight of the use of powers

There is no judicial oversight of the use of the powers outlined.

Article 63 of the Telecommunications Law states that the employees of ictQATAR who are vested with powers of judicial seizure by a decision from the Attorney General, following the agreement by the Chairman of the Board of ictQATAR, shall seize and prosecute offences committed in violation of the rules of the Telecommunications Law.

Censorship-related powers

In this section, we refer to Decree Law No. (34) of 2006 on the promulgation of the Telecommunications Law (Telecoms Law) and No. (1) of 2009 on the promulgation of the Executive By-Laws for the Telecommunications Law (Telecoms By-Laws).

1. Shut-down of network and services

National security or public emergency

Under Article 59 of the Telecoms Law, service providers (such as Vodafone) must comply with the requirements of any government department where such requirements relate to national security or a general public emergency. It is feasible that Vodafone could be required to shut down its network or services.

CRA licensing

Each network provider operates under a licence. Articles 3, 4 and 12 of the Telecoms Law and Article 15 of the Telecoms By-Laws provide that ictQATAR and Qatar's

Qatar

Communications Regulatory Authority (CRA) may suspend, revoke or refuse to renew a network provider's licence where the provider has repeatedly breached the Telecoms Law or the terms of its licence, or has not paid its licence fees. However, before making such a decision, the CRA should give a network provider a reasonable amount of time (such period of time to be determined by the CRA) to remedy its breach or the circumstances giving rise to the suspension, revocation or refusal to renew. Vodafone may therefore lose its licence to provide a mobile network, and related services, if Vodafone repeatedly breaches the terms of its licence.

2. Blocking of URLs and IP addresses

See 'Shut-down of network and services' above. It is feasible that Vodafone could be required to block certain URLs, IP addresses and/or IP ranges by a government department pursuant to the department's powers under Article 59 of the Telecoms Law.

3. Power to take control of Vodafone's network

See 'Shut-down of network and services' above. It is feasible that a government department using its powers under Article 59 of the Telecoms Law could take control of Vodafone's network.

4. Oversight of the use of powers

There is no judicial oversight of the government's use of its powers.

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes. Article 59 of Decree Law No. (34) of 2006 on the promulgation of the Telecommunications Law states that 'Service providers must comply with the requirements of the security authorities in the state which relate to the dictates of maintaining national security and the directions of the governmental bodies in general emergency cases and must implement orders and instructions issued by the General Secretariat regarding the development of network or service functionality to meet such requirements.'

In all cases involving national security and general emergency, the government agencies and LEAs can directly approach the service provider to decrypt customer data that it has encrypted. We are of the view that Decree Law No. 24, in particular the articles listed under this section, are wide enough to permit the government the legal authority to require the telecommunications operator to decrypt communications data where the telecommunications operator has applied the encryption.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

Article 59 of the Telecommunications Law would also apply to this scenario.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

While there is no express law on this matter, it is our view that a telecommunications operator cannot offer end-to-end encryption on its communication services without breaching the above-mentioned articles found in our answers to Questions 1 and 2. It would be advisable to liaise with the Ministry of Interior and the Ministry of Transportation and Telecommunications to obtain their opinion prior to launching such a service.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

We are not aware of any such examples. It should be noted that there is no doctrine of binding precedent in Qatar (so it is not possible to predict the course the court may adopt in the future) and that decisions of the Qatari courts are not published.

Romania

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

Council of Europe Convention on Cybercrime

By Law No. 64/2004, Romania has ratified the Council of Europe Convention on Cybercrime (ETS No. 185, 23 November 2001). Since that ratification, Romanian national laws have been amended so as to comply with the requirements of the convention regarding the collection, search, seizure, making available and interception of data.

Law No. 506/2004

According to Article 4 of Law No. 506/2004 on personal data processing and privacy protection in the electronic communications sector, the interception or surveillance of communications and related traffic data may be made only by the relevant public authorities as set out in the applicable statutory provisions or by the parties to the communications, unless the latter have consented in writing to the interception or surveillance being made by other parties.

Law No. 51/1991

Interceptions may be made on the request of intelligence and security agencies under Article 15 of Law 51/1991 where there are threats to the national security.

Law No. 14/1992

According to Article 8 of Law No. 14/1992 on the Romanian Intelligence Service organisation, the National Interceptions Centre is legally empowered to ensure the relevant enforcement authorities have the technical permits to execute the technical surveillance warrants.

Criminal Procedure Code

The following rules under Article 139(1) of the Criminal Procedure Code (Law No. 135/2010) regarding technical surveillance apply in relation to prosecuting certain categories of crime:

a. there is a reasonable suspicion that a serious crime is planned or has been committed;
b. the measure taken is proportionate to the restriction of the rights and freedoms that it entails; and
c. the relevant evidence could not be obtained otherwise or there is a danger for the safety of persons or valuables.

Furthermore, interceptions may be made based on warrants issued by the relevant court of law for a period of 30 days, which can be subject to further 30-day extensions granted by the court up to a total overall period of six months.

In exceptional cases, the prosecutor's office may directly authorise the interception by order for no more than 48 hours (Article 141(1) and (2) of the Criminal Procedure Code). The relevant prosecutor's office is to apply for the court's confirmation of the interception within no more than 24 hours of the expiry of an interception order (Article 141(3) and (4) of the Criminal Procedure Code).

According to Article 142(2) of the Criminal Procedure Code (Law 135/2010), the service provider is to cooperate with the prosecutor's office and the relevant authorities in order to enforce the technical surveillance (interception) warrants issued by the court.

ANCOM Decision No. 987/2012

According to Article 3.8 of Annex No. 1 to Decision No. 987/2012 of the National Authority for Management and Regulation in Communications (**ANCOM**) on the general authorisation for the provision of electronic communications networks and services, the service provider is inter alia obliged to:

i. technically allow the relevant authorities to perform interceptions and to make available all technical data regarding interceptions, in the format established by the authorities;
ii. duly cooperate with the relevant authorities involved in interceptions and ensure the confidentiality of interception operations;
iii. cooperate with the relevant authorities to implement security and audit criteria regarding the national communications interception system developed by them;
iv. take all necessary technical measures to enable interceptions in general and immediately enable the enforcement of interception warrants in particular;
v. place at the disposal of the relevant authorities the interception management servers and the administration and operation consoles it holds, as required to ensure interceptions; and
vi. bear the costs of the interception interface.

Romania

As per Article 8(2)(k) of the Government Emergency Ordinance No. 111/2011 on electronic communications, the conditions under which service providers are to bear the costs related to the interception interface are established by the general authorisation issued by ANCOM to the service provider.

2. Disclosure of communications data

Council of Europe Convention on Cybercrime

With Law No. 64/2004, Romania has ratified the Council of Europe Convention on Cybercrime (ETS No. 185, 23 November 2001). Since that ratification, Romanian national laws have been amended to comply with the requirements for the collection, search, seizure, making available and interception of data.

Law No. 82/2012

Decision No. 440 of 8 July 8 2014, issued by the Romanian Constitutional Court, has been published in the *Official Gazette* Part I No. 653 of 4 September 2014. On grounds of unconstitutionality, the decision repealed Law No. 82/2012 on the retention of data generated and processed by providers of electronic communications network or service.

Law No. 506/2004

Law No. 235/2015 amending and supplementing Law No. 506/2004 on personal data processing and the protection of privacy in electronic communications was published in the *Official Gazette* Part I No. 767 of 14 October 2015.

According to Article 5(1) of Law No. 506/2004 as amended, traffic data for customers should be deleted or turned into anonymous data when the customers do not serve any more to a communications delivery, but not later than three years after the communications.

According to the newly introduced Article 121(1) of Law No. 506/2004, communications providers may be obliged to provide data regarding traffic, equipment identification and localisation on request of the courts of law, criminal investigation bodies and national security agencies, subject to prior authorisation from the relevant court.

If the request is made by national security agencies, the procedures set out in Articles 14, 15 and 17–23 of Law No. 51/1991 regarding Romania's national security are to be observed, as detailed in Section 3 below.

According to Article 121(1), data disclosed as a result of such a request may not be erased or made anonymous by communications services providers if that is specified by the authority that has made the request, until the reasons that grounded the disclosure request have ceased and not more than five years after the date of the request or until the date of a final and binding court decision. The relevant authority must inform the communications services providers when the reasons that grounded the request have ceased.

Criminal Procedure Code

Communications service providers have an obligation to disclose traffic and location data, according to Article 152(1) of the Criminal Procedure Code (Law No. 135/2010).

The latest wording of Article 152, amended 2 May 2016 by Law No. 75/2016 on the approval of the Government Emergency Ordinance No. 82/2014 on the amendment and supplementation of Law No. 135/2010 of the Criminal Procedure Code, states that a prosecutor may, based on previous court approval, order communications providers to disclose traffic and location data, when all the following conditions are fulfilled:

i. there are reasonable suspicions regarding the perpetration of one of the crimes that are expressly listed in letter paragraph (1) letter a) of Article 152;
ii. there are justified grounds to consider the data as evidence;
iii. the evidence cannot be obtained in any other way or its collection could prejudice the investigation or endanger persons or valuable goods; and
iv. the measure limits the subject's fundamental rights, given the particularity of the case, in proportion to the importance of the information or of the evidence that is to be obtained, or the gravity of the crime.

Under Article 138 of the Criminal Procedure Code (Law No. 135/2010), criminal prosecution bodies may access any computer system, either directly or by means of specialised software or networks, and may intercept any type of communication in order to identify evidence, where:

i. there is a reasonable suspicion about a serious offence/crime;
ii. the measure is in proportion to the restriction of the rights and freedoms that it entails; and
iii. the relevant evidence could not be obtained otherwise or there is a danger for the safety of persons or valuables.

According to Article 139(1) of the Criminal Procedure Code (Law No. 135/2010), access to computer systems requires a warrant to have been issued by the court.

In exceptional cases, the prosecutor's office may directly authorise the access by order for no more than 48 hours (Article 141(1) and (2) of the Criminal Procedure Code).

According to letter b1) of Article 523 paragraph (1) of the Criminal Procedure Code (Law No. 135/2010), newly introduced by Law No. 75/2016 referred to above, communications providers may be requested to provide traffic and location data based on a court warrant throughout the procedures aiming to locate fugitives from justice. In accordance with Article 524, amended by the same Law No. 75/2016, the disclosure of such data may be made on the request of the relevant prosecutor if the relevant court finds that the identification, searches,

Romania

localisation and finding of the fugitive cannot be made by other means or would otherwise be substantially delayed.

Civil Procedure Code

According to Article 297(1) of the Civil Procedure Code, in civil and commercial trials the court may issue orders for third parties holding relevant information to present it in court if it is necessary for the settlement of the case.

3. National security and emergency powers

Article 13 of Law No. 51/1991 regarding Romania's national security states that national security agencies may request communications data generated or processed by communications providers (other than the content of these communications) and retained by them under the law. Instances where communications providers may retain communications data are scarce and strictly regulated.

According to the newly introduced Article 121 of Law No. 506/2004 on personal data processing and privacy protection in the electronic communications sector, traffic data, equipment identification data and location data are to be disclosed among other on request of national security agencies in accordance with the legal provisions on data privacy, and subject to the procedure set out in Articles 14, 15 and 17-23 of Law No. 51/1991.

This disclosure may not be requested unless:

i. the following conditions are fulfilled:
   a. there is no alternative way to learn about, prevent and counteract risks or national security threats;
   b. the measures are necessary and proportional given the circumstances of the case; and
   c. the authorisation provided by the law has been obtained; and
ii. an express authorisation and a warrant issued by the High Court of Cassation and Justice (Romania's supreme court), on request of the prosecutor's office attached to said court, are obtained; in exceptional cases (ie when a delay would severely prejudice the purpose of the envisaged activities) the authorisation may be issued by the prosecutor for a maximum of 48 hours, after which a court authorisation must be obtained.

Data disclosed following such a request may not be erased or made anonymous by communications services providers if so specified by the national security agency that has made the request, until the reasons that grounded the disclosure request have ceased and not more than five years since the date of the request or until the date of a final and binding court decision, as the case may be. The relevant agencies are to inform the communications services providers when the reasons that grounded the request have ceased.

Article 24 of Law No. 51/1991 also sets a general obligation for all public and private sector actors to provide support to national security agencies and allow them access to data held that may have an impact on national security. Nonetheless, insofar as communications services providers are concerned, such access should be deemed subject to the limitations and procedures described above.

Under Articles 1 and 3(c) of Law No. 132/1997 on requisitions, under exceptional circumstances (eg war, national emergency and disasters) public authorities and national defence forces can take temporary possession of any goods in order to gain access and use of the telecommunications systems.

According to Law No. 132/1997, the following instruments are required to requisition the assets of telecommunications networks:

i. a requisition plan drawn up by the local authorities before the relevant events occur (Article 5(2)); and
ii. a military order for hand-over to be issued at the date of the actual requisition (Article 13).

According to Article 18 of Government Emergency Ordinance No. 34/2008 on the National System for Emergency Calls, the providers of electronic communications are obliged to make available, free of charge, to the director of the National System for Emergency Calls an updated database with all telephone numbers, names and addresses of customers.

According to Article 20 of Government Emergency Ordinance No. 1/1999, during a state of siege or emergency, exceptional measures established by military authorities will be enforced via military orders that are mandatory throughout the country.

4. Oversight of the use of powers

In addition to those set out above, the following rules relate to remedies that may be sought following the use of these powers:

a. cost conditions related to an interception interface are to be borne by the service provider and may be challenged in court via administrative litigation; and
b. requisition measures may be challenged in court only with respect to the amount of the compensation.

Romania

Censorship-related powers

1. Shut-down of network and services

Government Emergency Ordinance No. 111/2011

The Government Emergency Ordinance No. 111/2011 gives the telecom regulatory authority, ANCOM, the power to shut down Vodafone's network or services (temporarily or permanently) in certain circumstances.

Article 9(2) of the same act provides that ANCOM may withdraw a general authorisation from a service provider where necessary in light of an international agreement entered into by Romania or required to protect the public interest. Under Article 135(1), withdrawal of the general authorisation may be made only after the decision is subjected to public debate; this consists of one or more public sessions where members of the industry, civil organisations and other relevant authorities are invited to submit their observations on the proposed measures; observations expressed during the public debate must then be observed by ANCOM.

Under Articles 147 and 148, ANCOM may revoke a service provider's right to supply networks or certain communications services for between six months and three years and/or remove the service provider's right to use numbering resources, radio frequencies and other technical resources:

- where that service provider has failed to comply with any of the terms of its general authorisation, frequency or licence numbering; or
- if it has failed to comply with certain obligations regarding monitoring spectrum usage, numbering resources or providing financial documents.

Under Article 141(1) ANCOM must notify the service provider before revoking or suspending its right to supply networks or communications services, or revoking or suspending its right to use numbering resources, radio frequencies or other technical resources.

2. Blocking of URLs and IP addresses

Law No. 196/2003

Article 11(2) of Law No. 196/2003 provides that ANCOM may require an internet service provider, such as Vodafone, to block the URL or IP address of websites containing illicit content. Illicit content is pornographic content which lacks an appropriate age restriction warning or which contains child sex abuse, bestiality or necrophilia.

Government Emergency Ordinance No. 77/2009

Article 10(7) of Government Emergency Ordinance No. 77/2009 on gambling provides that network and internet service providers are obliged to comply with the decisions of the Gambling Monitoring Authority with respect to blocking access to unauthorised gambling websites in Romania.

3. Power to take control of Vodafone's network

Law No. 132/1997

Under Articles 1 and 3(c) of Law No. 132/1997, in exceptional circumstances public authorities and national defence forces can take temporary possession of any network assets in order to gain access to and use of a telecommunications network. Exceptional circumstances would be a national emergency such as a natural disaster or war. According to Article 5(1)(c), when making a requisition, a local authority must present its requisition plan (drawn up before the relevant events occur) and, where the requisition is made by national defence forces, the relevant force must present a military order for the possession of network assets issued at the date of the actual requisition.

Law No. 255/2010

Law No. 255/2010 enables public authorities to take possession of any type of land or building if this is required for public utility reasons. In order to expropriate the land or building, a decision of the government or local administration, setting out the details of the seizure and the amount of compensation to be awarded, must be presented.

4. Oversight of the use of powers

All decisions made by ANCOM or the Gambling Authorisation Commission can be challenged in court by administrative litigation proceedings.

Where a public authority or military force takes control of Vodafone's network in accordance with Law No. 132/1997 or Law No. 255/2010, the party subject to requisition or expropriation may challenge in court the amount of compensation received for their losses arising from such expropriation, but not the decision itself to expropriate.

Romania

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

The current legislation does not contain provisions explicitly requiring communications service providers (CSPs) to decrypt communications data. Nonetheless, such an obligation could be inferred from the various legal provisions enshrining general law enforcement assistance obligations to allow interception of communications content or to provide various other data.

Regarding the interception of content (see 'Provision of real-time lawful interception assistance' earlier in this chapter), Article 142 (2) of the Criminal Procedure Code provides an obligation for CSPs to cooperate with prosecutors and criminal investigation bodies, to the best of their capabilities, in order to execute technical surveillance warrants. Likewise, Article 3.8 of Decision No. 987/2012 of ANCOM sets out an obligation for CSPs to allow competent authorities to perform interceptions, as well as to make all technical data regarding interceptions available, to provide technical support in intercepting communications and, in general, to take all technical measures necessary to immediately execute interception warrants. It may, therefore, be inferred that interception should offer access to the decrypted version of the content, where the ability to decrypt is within the CSP's technical competence (by holding the encryption key).

Regarding traffic and location data processed by CSPs (see 'Disclosure of communications data' earlier in this chapter) – in particular Articles 152; Articles 523–524; and Article 170(2) of the Criminal Procedure Code – it may be argued that where a CSP holds the encryption key, the traffic and location data it is legally obliged to provide should be decrypted so that the disclosure is effective.

Finally, there are other legal provisions, such as those concerning powers of national security or competition authorities, regulating in an equally broad manner such authorities' rights to access certain types of data. These legal powers may apply in this context as well, depending on the scenario.

With a lack of any meaningful court practice on the matter to date, opinions between criminal law practitioners on the subject are, however, divided, there being also voices who hold the view that there are no legal grounds at present to support a decryption requirement.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

As described in detail above, the statutory law on law enforcement (Law No. 135/2010 regarding the Criminal Procedure Code) as well as other laws enshrining various rights to access data in favour of national security agencies and other authorities, contains no explicit provision regarding the legal authority of the government to order CSPs to decrypt data, whether encrypted by the CSPs themselves or by third parties.

However, to the extent that decryption of the data is within a CSP's competence or control, and based on existing general provisions, it may be argued that the CSP should proceed to decryption when requested to ensure access to certain data.

With a lack of any meaningful court practice on this subject to date, opinions among criminal law practitioners are, however, divided, some favouring the view that there are no legal grounds at present to support a decryption requirement.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

Under existing legislation, there is no explicit provision prohibiting a CSP from offering end-to-end encryption on its communications services.

Under the circumstances, this question should be considered from two angles, as follows.

Firstly, it should be considered whether, when facing a specific request for disclosure of encrypted data, the CSP would be also required to decrypt it. Arguably, as described in Questions 1 and 2 above, to the extent that decryption is within the CSP's technical capabilities, a decryption request might be considered as grounded. However, to the extent that the decryption is not within CSP's technical reach and capabilities, the risk that a decryption request (that is filed based on the general obligations of access to the data concerned described at Question 1) might be considered as grounded should be considerably smaller.

Romania

Secondly, it should be considered whether the fact that a CSP is setting up an end-to-end encryption service would, as a direct consequence, make it impossible to effectively enable the relevant authorities to access the data that they are entitled to request. This itself could be deemed a breach of the laws mentioned at (A) and (B).

Regarding the provisions of the statutory law on law enforcement, the risk should be remote, as long as the decryption is not within the CSP's competence and technical capability.

Moreover, even if one could deem that failure to decrypt the data or failure altogether to provide data in a readable form, might amount to a breach of the CSP's law enforcement related obligations, as a matter of principle this should not be considered as a criminal offence.

Likewise, setting up a service of end-to-end encryption while being aware that it may be used by persons perpetrating criminal offences should not by itself trigger a CSP's criminal liability.

This is because the criminal offences concerned (ie the obstruction of justice, regulated by Article 271 of Law No. 286/2009 of the Criminal Code and the support to a person committing criminal offences, regulated by Article 269 of the Criminal Code) require, in principle, a direct intention on behalf of the CSP. In other words, in order to commit such offences, CSP would have to provide end-to-end encryption with the direct purpose of obstructing justice and of helping those who commit criminal offences.

Regarding the provisions of the communications legislation, these state, among other things, as mentioned in Questions 1 and 2, that a CSP is to provide support to relevant authorities and take all requisite technical measures to ensure that the interception of a communication takes place. Such a general obligation could eventually be construed as requiring the telecommunications operator to provide or ensure effective access, namely access to decrypted information. However, it may be argued that by setting up an end-to-end encryption service, the CSP has deliberately put itself in a position not to properly observe the said obligations, and thereby that it has breached them.

According to Articles 142 and 143 of Government Emergency Ordinance No. 111/2011 regarding electronic communications, such a breach could be sanctioned with a fine amounting to 2% of the company's annual turnover (and 5% in case of repeated breaches), whenever a company's annual turnover exceeds RON3,000,000 (the approximate equivalent of EUR660,000).

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

Based on publicly available information, there is no case where the government has used legislation predating the advent of commercial encryption to produce judgments that were consequently applied to its use.

Considering that all Romanian legislation previous to 1990 providing the government with powers similar to those granted to American authorities under the All Writs Act (ie national security legislation) has been abolished and replaced by new legislation during the 1990s, such a situation is unlikely to occur.

South Africa

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

The Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002

The Regulation of Interception of Communications and Provision of Communication-Related Information Act No.70 of 2002 (**RICA**) states that the interception and monitoring of communications is prohibited unless:

- a directive has been granted that permits the prohibited activities;
- the party protected by RICA gives requisite consent;
- the entity engaging in the activity was also a party to those communications;
- it is to intercept, monitor or disseminate information of an employee while carrying on a business;
- it is to prevent serious bodily harm;
- it is to determine a location during an emergency; or
- if entitled to do so in terms of other legislation.

An interception direction can only be issued if a judge is satisfied that a serious offence has been or will be committed, or the gathering of information is necessary due to an actual threat to public health or safety, national security or compelling national economic interests of the Republic.

Chapter 3 of RICA sets out circumstances under which an applicant may apply for an interception and monitoring direction and entry warrants along with the manner in which such directions and entry warrants are to be executed.

Section 16 of RICA states that an applicant may apply in writing to a designated judge for an interception direction where there are reasonable grounds to believe that a serious offence has been, is being or will probably be committed, or in order to gather information concerning an actual or potential threat to public health or safety, national security or compelling national economic interests. In terms of Section 22, the applicant may simultaneously apply for an entry warrant.

Section 21 of RICA provides for the issuing of decryption directions by application to a designated judge.

Oral applications for any direction or warrant listed above may be made in terms of Section 23 of RICA.

Section 30 of RICA states that a telecommunications service provider must provide a telecommunications service which has the capability to be intercepted and store communication-related information. A directive sets out:

i. the capacity needed for interception purposes;
ii. the technical requirements of the systems to be used;
iii. the connectivity with interception centres;
iv. the manner of routing duplicate signals of indirect communications to designated interception centres; and
v. the manner of routing real-time or archived communication-related information to designated interception centres.

2. Disclosure of communications data

RICA requires a telecommunications service provider to intercept and store communication-related information which is commonly referred to as metadata.

Section 17 of RICA provides for the issuing of a real-time communication-related direction. This is required where no interception direction has been issued and only real-time communication-related information on an ongoing basis is required. An applicant may apply to a designated judge for the issuing of the direction.

Section 19 of RICA provides for the issuing of an archived communication-related direction. If only archived communication-related information is required, an applicant may apply to a high court judge, a regional court magistrate or a magistrate for the issuing of this direction.

3. National security and emergency powers

Except as set out above, the South African government does not have any legal authority to invoke special powers in relation to access to a mobile network operator's customer data and/or network on the grounds of national security.

South Africa

4. Oversight of the use of powers

As detailed above, applications under RICA may be made to a designated judge, high court judge, regional court magistrate or magistrate as necessary. A 'designated judge' refers to any judge of a High Court discharged from active service under Section 3(1) of the Judges' Remuneration and Conditions of Employment Act No. 47 of 2001 or any retired judge who is designated by the Minister of Justice to perform the functions of a designated judge for the purposes of the act.

To maintain interception capability as required under Section 30 of RICA, no judicial oversight of the requirements is issued. The cabinet member responsible for communications, together with the Minister of Justice after consultation with the Independent Communications Authority of South Africa and the telecommunications service provider/s concerned, must, on the date of the issuing of a telecommunications service licence, issue a directive as detailed above.

Censorship-related powers

1. Shut-down of network and services

There is no national security legislation that empowers the government to order a blanket shut-down by network providers of their network or communications services.

However, subject to compliance with the provisions of Section 37 of the Constitution, the government may, after declaring a state of emergency, implement measures that derogate from the protection afforded under the Bill of Rights. Such measures may include derogation from the guaranteed right to receive and impart information or ideas as set out under Section 16(1)(b) of the Constitution. Moreover, such measures can include the order for the suspension of communications services. A state of emergency can only be declared through an Act of Parliament and only where the nation is threatened by war, invasion, disorder, natural disaster or other forms of public emergency, or where the declaration is necessary to restore peace and order. States of emergency are measures of last resort and can be justified only by an exceptional crisis which affects the whole population and constitutes a threat to the organised life of the population; the mere existence of disorder or unrest is not sufficient.

The Electronic Communications Act No. 36 of 2005 (the **EC Act**) and the Independent Communications Authority of South Africa Act No. 13 of 2002 (the **ICASA Act**) empower the Authority to suspend or cancel an individual network provider's licence (such as Vodacom's) in specific instances. Such a suspension or cancellation would mean that the affected licensee would be unable to provide its network or services – it would effectively shut them down. It can only be directed at an individual licensee due to its non-compliance with regulatory requirements; it cannot be a blanket order to all network provider licensees, even during periods of unrest or emergency.

A law enforcement authority can also, at any time, seek a court-ordered subpoena to require a network provider to shut down its network or services.

2. Blocking of URLs and IP addresses

It is feasible that network providers (such as Vodacom) might be requested to block certain URLs or IP addresses. However, no such request has been made to date.

3. Power to take control of Vodacom's network

The government does not have the legal authority to take control of Vodacom's network. It is hypothetically possible that the powers exercised by the government during a state of emergency might amount to taking control of a network provider's network, but this is without precedent.

4. Oversight of the use of powers

A network provider may submit a complaint about a request made to it by the government or a law enforcement authority, including during a state of emergency, to the Inspector General of Intelligence. The Inspector General of Intelligence oversees the activities of law enforcement authorities, such as intelligence agencies and the police. Upon a complaint being made by a network provider, the Inspector General would investigate and provide an opinion as to whether that network provider should comply with the request or not.

Each court-ordered subpoena contains a date at which a court hearing will take place. Should the network provider subject to the court order decide to challenge the subpoena (including the obligation to comply with it), it can do so at the scheduled court hearing.

South Africa

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes.

The Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002 (RICA) requires a telecommunications service provider to decrypt encrypted communication in limited circumstances. Section 21 of RICA states that an applicant may apply to a designated judge for the issuing of a decryption direction during, or at any stage after, the issuing of the interception direction. A 'designated judge' refers to any high court judge discharged from active service under Section 3(1) of the Judges' Remuneration and Conditions of Employment Act No. 47 of 2001 or any retired judge who is designated by the Minister of Justice to perform the functions of a designated judge for the purposes of the act.

The government can require the telecommunications operator to decrypt communications data where the telecommunications operator has applied the encryption under RICA.

Section 16(1) of RICA provides that 'An applicant may apply to a designated judge for the issuing of an interception direction…'.

Section 21(1) of RICA provides that 'An applicant who:

a. makes an application referred to in Section 16 (1) may in his or her application also apply for the issuing of a decryption direction; or
b. made an application referred to in Section 16 (1) … may … apply to a designated judge for the issuing of a decryption direction….'.

Section 21(2) provides that '… an application referred to in subsection (1) must be in writing and must:

a. indicate the identity of the
   i. applicant
   ii. decryption key holder to whom the decryption direction must be addressed'.

A decryption key holder is defined as 'any person who is in possession of a decryption key for purposes of subsequent decryption of encrypted information relating to indirect communications'.

Note that a decryption order can only be sought in certain circumstances – broadly they would be those set out earlier in this chapter where law enforcement assistance is required.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

Where the telecommunications operator is not the decryption key holder, but has the technological ability to 'unlock' the communications data, then the government may make an application in terms of Section 21(2) of RICA which provides that:

'(c)…, an application referred to in subsection (1) must be in writing and must specify the:

i. decryption key, if known, which must be disclosed; or
ii. decryption assistance which must be provided, and the form and manner in which it must be provided'.

Decryption assistance is defined in RICA as meaning to:

'(a) allow access, to the extent possible, to encrypted information; or

(b) facilitate the putting of encrypted information into an intelligible form;…'.

Where the telecommunications operator is the decryption key holder, the government may follow the process in Section 21(1) of RICA, as discussed in the answer to Question 1 above.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

Yes, a telecommunications operator can offer end-to-end encryption software on its communication services, even if it has not been able to decrypt the encrypted communication data.

Section 30 of RICA, as mentioned above in Question 2, imposes on a telecommunications operator only the obligation to provide a telecommunications service that is capable of interception, and interception does not impose an obligation to decrypt communications data.

In such a case, the holder of the decryption keys would be the customer and not the telecommunications operator. In terms of Section 29(1) of RICA, the government may, in the execution of the decryption direction, obtain assistance from the decryption key holder who is not a telecommunications service provider to decrypt communications data. Therefore, application for a decryption direction can be made in relation to the customer directly.

South Africa

The answer would not differ if the question applied to the provision of 'business as usual' communication services (where the communication routes over the network as a data packet) or 'over the top' communication services (where the delivery of a communication is made via Internet Protocol (IP) over the network) by the telecommunications operator.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

In South Africa, prior to the promulgation of RICA, interception of communications was governed by the Interception and Monitoring of Prohibition Act 127 of 1992 (**IMP Act**). The IMP Act has been repealed by RICA.

The case law determined under, and which was reliant upon, the IMP Act cannot be used as a foundation for any judgment today as the enabling legislation has been repealed. In any event, many provisions of the IMP Act would be found to be unconstitutional post-1994 and therefore unlawful.

Spain

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

Service providers and operators of public electronic communication networks may be required to intercept communications in the following scenarios:

Criminal Procedure Act

a. A judge may, either ex officio or following an initiative by the judicial police or Public Prosecutor, issue an interception order if the criminal investigation for which a court authorisation is requested is carried out in relation to the prosecution of:
   - one of the criminal offences referred to in Article 579.1 of the Criminal Procedure Act and approved by the Royal Decree of 14 September 1882 that was later modified by the Act 13/2015 of 5 October to strengthen procedural safeguards and regulate the technological investigation measures which entered into force in December 2015 (the **Criminal Procedure Act**); or
   - other criminal offences perpetrated through an IT-based instrument or any other information or communications technology or communications service.

Requests for a court authorisation must contain the legal requirements set out by Article 588 bis b in relation to Article 588 ter d of the Criminal Procedure Act.

b. The Criminal Procedure Act states (according to Article 588 ter d3) that in cases of urgency, when the investigations are carried out in the context of the prosecution of criminal offences related to the activities of armed gangs or terrorist elements, the interception of communications may be ordered by the Minister of Home Affairs (Ministro del Interior), or by the Secretary of State for Homeland Security. In such cases, the measure has to be communicated within 24 hours. A reasoned opinion must be made in writing to the relevant judge, who will revoke or confirm it, also with a reasoned opinion, within 72 hours of when the measure was ordered.

c. Article 588 ter e of the Criminal Procedure Act obliges all providers of telecommunication services, providers of access to a telecommunications network or information society services to assist and collaborate with the judge, the Public Prosecutor or the agents of the judicial police to ensure compliance with the interception orders, while maintaining secrecy about the measures required. Failure to do this may lead to an offence of disobedience.

Act 2/2002 of 6 May on prior judicial control applicable to the National Intelligence Centre

d. According to Act 2/2002 of 6 May on prior judicial control as applied to the National Intelligence Centre, the National Intelligence Centre (CNI) may ask the operator to intercept communications in cases where the Secretary of State-Director of the CNI has obtained an authorisation from a competent judge of the Supreme Court, in accordance with the specific requirements under such law.

e. In cases of justified urgency (based on the authorisation request submitted by the Secretary of State-Director of the CNI), the competent judge may confirm or deny the requested authorisation with a reasoned opinion issued within 24 hours (rather than the usual 72 hours).

The Universal Service Regulation

Articles 83 to 101 of the Regulation on the conditions for the provision of electronic communication services, the universal service and the protection of users, approved by Royal Decree 424/2005 of 15 April and modified by Royal Decree 726/2011 of 20 May (the **Universal Service Regulation**), determine the procedure and the measures to be adopted by service providers and operators of public electronic communication networks to intercept communications in cases where they are obliged to do so by law. The Universal Service Regulation establishes, among other things, the general requirements of the procedure, access requirements, the information to be delivered to the authorised agent (judicial police or CNI agent) and other operational requirements (previous information, locations, authorised personnel, confidentiality, real-time access, interception interfaces, etc).

A court order or an authorisation must be issued by the relevant judge **before** the interception takes place, except in case (b) outlined above.

Spain

Order ITC/110/2009

In addition, Order ITC/110/2009 of 28 January on the general framework applicable to the specifications to be followed for the legal interception of communications (**General Framework Order**) establishes the relevant technical requirements and interfaces to be implemented by service providers and operators of public electronic communication networks to carry out the interception of a communication.

General Telecommunications Act 9/2014 of 9 May

Article 39 of the General Telecommunications Act 9/2014 of 9 May (**LGTel**) sets out the operator's duty to intercept communications when required to do so by the relevant authorities through the appropriate interfaces and technical resources, that should be ready for this purpose. This Act, the Universal Service Regulation and the General Framework Order together provide a detailed description of the obligations of operators in terms of measures, procedures, interfaces and technical requirements to be put in place in order to comply with their interception duties.

In addition, there are further Orders which aim to regulate particular technologies, such as:

i. Order ITC/313/2010 of 12 February implementing and adapting the technical specification ETSI TS 101 671 on Lawful Interception (LI) and on the handover interface for the LI of telecommunications traffic; and

ii. Order ITC/682/2010 of 9 March implementing and adapting the technical specification ETSI TS 133 108 (3GPP TS 33.108) on the Universal Mobile Telecommunications System (UMTS), as well as 3G security and the handover interface for LI.

These laws do not appear to grant government and law enforcement agencies the legal powers to allow direct access into a communication service provider's networks without the operational or technical control or cooperation of the communications service provider.

2. Disclosure of traffic data

Data Retention Act 25/2007

Act 25/2007 of 18 October on data retention related to electronic communications and public communication networks (**Data Retention Act**) regulates:

i. the operator's obligation to retain traffic and localisation data, as well as other necessary data to identify the user (traffic data) generated or processed in the provision of electronic communication services or public communication networks; and

ii. the duty to transfer such traffic data to the relevant agents whenever they are required to do so, through the relevant court order or judicial authorisation. In addition to the judicial police and CNI agents, the Data Retention Act explicitly includes the staff members of the Office of Customs Surveillance as authorised agents in this regard.

The Data Retention Act, among other things, regulates the traffic data to be retained, the obligation to store traffic data, the period of time during which such traffic data must be stored or retained by the operator, the procedure and security measures involved in the transfer of the traffic data to the relevant agents, and the sanctions to be imposed on operators that do not comply with such obligations.

The content of the communications is explicitly excluded from the scope of this Act.

In accordance with Articles 6 and 7 of the Data Retention Act, operators have the obligation to disclose the retained data to the authorised agents (see above), following the instructions contained in a court order issued by the relevant judge and according to the provisions of the Criminal Procedure Act and the principles of necessity and proportionality.

Act 13/2015 that modifies the Criminal Procedure Act

On December 2015, Act 13/2015 of 5 October which modified the Criminal Procedure Act entered into force stating that electronic traffic or associated data retained by service providers may only be disclosed for inclusion in the process by a court order. When such information contained in a service provider's automated archives is deemed indispensable for the ongoing investigation, the appropriate authorisation must be requested from the competent judge.

In addition to this, either the Public Prosecutor or the judicial police may require any legal person to retain and protect certain data or information in a computerised storage system until the appropriate court order authorising its disclosure is obtained. The maximum timeframe for this retention cannot be more than 180 days.

Moreover, Articles 588 ter k, 588 ter l and 588 ter m set out the conditions for accessing non-traffic data without a court order, provided this is necessary for the purposes of identifying users, terminals and connected devices, and as long as the applicable requirements are met. In this sense:

i. Article 588 ter k concerning 'Identification through IP number' states that whenever the agents of the judicial police have access to an IP address used to commission a crime, they may ask the competent judge to prompt the subjects under the assistance and collaboration duties of Article 588 ter e, to disclose the data allowing them to identify and localise the terminal or connected device and also identify the suspect;

ii. according to Article 588 ter l, in the context of a criminal investigation, the agents of the judicial police may use technical tools to gain access to identification codes or technical tags

Spain

belonging to a communication device or any of its components (eg IMSI or IMEI numbers), provided that the subscriber's number could not be obtained and it is deemed indispensable for the purposes of the investigation; and

iii. under Article 588 ter m, whenever the Public Prosecutor or the judicial police, in the exercise of their functions, need to know the ownership of a telephone number or of any other means of communication, or conversely, require the telephone number or the identifying data of any means of communication, they may address the provider directly and such provider will be obliged to provide that information.

3. National security and emergency powers

According to Article 4.6 of the General Telecommunications Act (LGTel), the government may, exceptionally and temporarily, enable the General Administration to take over direct management of certain services or exploit certain electronic communications networks in order to ensure public safety and national defence.

Moreover, on the basis of a breach of public service obligations (under the Title III General Telecommunications Act), the government, following a mandatory report from the telecoms regulatory authority (CNMC), may also, exceptionally and temporarily, enable the General Administration to take over the direct management of the services or exploit corresponding networks. Regarding the latter, it may also, under the same conditions, intervene in the provision of electronic communications services.

According to the exceptional regulations provided by Act 4/1981 of 1 June on the states of alarm, emergency and siege (**LSAES**):

- during a state of alarm (in the case of essential goods running out in the whole of Spain or in a certain region – Article 4.d), the government may issue necessary orders (Article 11.e) or decide to intervene in those services or mobilise its personnel (Article 12.2) in order to ensure the functioning of the affected services;
- during a state of emergency (which may be requested because of a serious alteration of essential public services or for other reasons), the government may intercept any kind of communications provided this is necessary to clarify alleged criminal offences or to maintain public order (Article 18); and
- during a state of siege, the government directing military and defence policies will assume all exceptional prerogatives (Article 33.1).

The declaration of a state of alarm will be conducted by decree by the government.

Once the government has obtained an authorisation from the Congress, it will declare a state of emergency by decree. The authorisation must include the suspension of Article 18.3 of the Constitution, that relates to the secrecy of communication, in order for Article 18 LSAES to be applied.

The government proposes a declaration of state of siege before the Congress.

In addition, Article 8.2 of Act 34/2002 of 11 July on information society services and electronic commerce (**LSSI**) states that in order for the competent authorities to identify an alleged infringer, they may ask information society service providers (ISSPs) (which may include telecommunications operators) to disclose data which would permit such identification. This request must be based on a previous judicial authorisation, in accordance with Article 122 bis of the Law 29/1998 of 13 July governing Administrative Jurisdiction (**LJCA**).

Article 122 bis of the LJCA refers to the necessary requirements that must be met in order to obtain judicial authorisation: an initial request by the competent authorities, that must include the pertinent reasons for the request and also the relevant documents. The court, within 24 hours from the request and once the Public Prosecutor has been heard, may issue the requested authorisation, provided that it will not affect Article 18 paragraphs 1 and 3 of the Constitution.

4. Oversight of the use of powers

In line with the Criminal Procedure Act, the relevant court order will determine the extension and scope of the disclosure to be carried out. The relevant judge has a duty of supervision to ensure compliance with such a court order.

The competent judge must be notified immediately and in reasoned writing of the intervention determined from Article 18 of the LSAES.

Spain

Censorship-related powers

1. Shut-down of network and services

Act 4/1981 of 1 June on the states of alarm, emergency and siege

Under Act 4/1981 of 1 June on the states of alarm, emergency and siege, certain constitutional rights are suspended and an exceptional legal regime is provided for those situations when Spain experiences one of these states. The most relevant to the shut-down of Vodafone's network and/or services are the powers which the government obtains when a state of alarm or siege is declared.

A state of alarm occurs when there is shortage of essential goods or services in either the whole of Spain or a certain region of it (for example, as a result of a general strike); it can only be declared by decree of the government that must report this state to the Congress (Parliament). Without this authorisation, the government cannot extend the initial period of 15 days. Under Article 11 of the LSAES, during a state of alarm, the government may intervene to remedy the shortage. It is feasible, therefore, that should a major issue arise in respect of Spain's communications, the government might intervene in relation to Vodafone's network. It is most likely that such an intervention would be used to improve or restore the affected network or communication service. However, it is possible that such an intervention could extend to closing the network or shutting the service down.

A state of siege occurs when the government is concerned with military and defensive policies related to protecting the national security. The government must submit its proposal before Parliament in order to declare a state of siege. During a state of siege, the government may assume all exceptional prerogatives which come with it – including the ability to order a shut-down of Vodafone's network or services.

General Telecommunications Act 9/2014 of 9 May

Articles 79 (sanctions) and 82 (interim measures in the framework of sanctioning proceedings) of the LGTel establish that the government or the telecoms regulatory authority, CNMC, may suspend (as an interim measure) or withdraw a network provider's right to provide electronic communications networks, services and/or utilities. They may only do so in the case of serious and repeated breaches by the network provider relating to service provision, network exploitation or the granting of usage rights, or specific conditions that the regulator has imposed on that operator, when previous measures to request the cease of the breach have been unsuccessful. The government and CNMC, therefore, have the power to shut down Vodafone's network or certain parts of Vodafone's services, but only if they deem Vodafone to have seriously or repeatedly breached its obligations as a network provider.

In addition, Article 28.1 of the LGTel, together with its complementary regulations (Articles 17 and 53 of the Royal Decree 424/2005), states that the government may, for reasons of national defence, public security or civil protection, impose other public service obligations that differ from the Universal Service Regulation.

2. Blocking of URLs and IP addresses

Act 34/2002 of 11 July on information society services and electronic commerce

Under Article 11.1, where a competent authority has found certain content to infringe the principles set out in Article 8.1, a court may order a network provider (such as Vodafone) to suspend access on its network to such content. In practice, Vodafone would do this by blocking the URL or IP addresses which link to the content being hosted. The principles set out in Article 8.1 include:

a. safeguarding public order, security and national defence;
b. protecting public health and consumers;
c. respecting fundamental rights (dignity, non-discrimination);
d. child protection; and
e. safeguarding intellectual property rights.

Copyright Act 1/1996

In connection with the Act above, the Copyright Act, approved by Royal Decree 1/1996 of 12 April and modified by Act 21/2014 of 4 November, developed the safeguarding of intellectual property rights over the internet by broadening the liability of intermediary service providers and increasing penalties for copyright infringement.

In particular, Section Two of the Copyright Commission represents the body in charge of the notice of takedown procedure against alleged copyright infringing activities by information society service providers (ISSPs) (eg blogs, websites) and ISSPs providing the description and location of presumably infringing works displayed on the website by means of an active contribution (not merely technical intermediation). Especially relevant is the fact that whenever ISSPs refuse to collaborate with the requests of the Copyright Commission over the removal of infringing content, intermediary service providers (such as Vodafone) may be required to suspend the services offered to such ISSPs.

To request a suspension of the service or the blocking of access to infringing resources, the Copyright Commission must be granted prior authorisation by a judge. In addition, in cases of serious infringements or where the social impact of the infringement is high, the ISSP may be required to cease its activities for a maximum of one year. To ensure the effectiveness of this measure,

Spain

the intermediary service providers may be requested (provided that the authorisation of a judge is obtained) to suspend the service provided to such ISSP. In both scenarios, and under the amended Copyright Act, the lack of cooperation with the Copyright Commission (ie not suspending the service) is regarded as a very serious infringement under the LSSI.

3. Power to take control of Vodafone's network

Act 4/1981 of 1 June on the state of alarm, emergency and siege

See 'Shut-down of network and services' above.

General Telecommunications Act

In principle, the LGTel allows the government, in a state of emergency or siege, to manage the telecommunications service as a 'temporal' public service. In particular, Article 4.6 (telecommunications services for national defence, public and traffic safety, and civil protection) of the LGTel states that the government may, exceptionally and temporarily, order the General Administration to assume direct management of certain electronic communications networks or services, in the interests of public safety or national defence.

4. Oversight of the use of powers

Act 4/1981 of 1 June on the state of alarm, emergency and siege

There is no judicial oversight of the specific emergency powers provided for when a state of alarm or siege is declared. The intervention determined according to Article 18 of the LSAES (state of emergency) must be notified immediately through a reasoned report to the competent judge.

General Telecommunications Act

There is no judicial oversight of the government's or CNMC's use of the powers provided for by the General Communications Act.

Copyright Act

In all cases, the enforcement of the collaboration measure issued to the relevant intermediation services provider requires prior authorisation by a competent judge in accordance with the procedure established under Article 122 bis LJCA.

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes. Under the first paragraph of Article 39 of the General Telecommunications Act 9/2014 of 9 May (LGTel), operators that exploit public electronic communication networks or make electronic communication services available to the public must guarantee the secrecy of such communications as set out in Articles 18.3 and 55.2 of the Constitution, and must adopt the necessary technical measures to do so. The second paragraph of Article 39 states that those operators are under an obligation to perform the interceptions authorised in accordance with the applicable Spanish laws and regulations.

Under Article 39.11 of the LGTel, where communications are subject to legal interception, compression, encryption, digitisation or other types of coding procedures, operators must deliver the communications free of the effects produced by such procedures, provided that they are reversible. Moreover, the intercepted communications must be provided to a quality no less than the one obtained by its recipient.

In addition, Article 43 of the LGTel establishes that any type of information transmitted through electronic communications networks may be protected by encryption procedures. Among the terms of use of such procedures, whenever they are used to protect the confidentiality of the information, a specific obligation may be imposed. This obligation consists of providing the General Administration or a public body with the algorithms or any encryption procedure used, as well as providing – free of cost – the encrypting devices to control them, under the applicable laws.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

Article 588 ter(e) of the Criminal Procedure Act, approved by Royal Decree of 14 September 1882 and later modified by Act

Spain

13/2015 of 5 October, for the strengthening of procedural safeguards and regulation of the technological investigation measures, which entered into force in December 2015 (SCPA), relates to:

i. all telecommunications services providers;
ii. telecommunications network access providers;
iii. information society service providers (ISSPs); and
iv. any other person who in any way contributes by facilitating communications through a telephone or any other computerised, logical or virtual device or system.

It obliges them to assist and collaborate with the criminal judge, the Public Prosecutor or the agents of the judicial police to enable the fulfilment of legal interception orders, while maintaining secrecy in relation to the measures required by the authorities. Failure to fulfil these duties may lead to an offence of disobedience.

Also, according to the exceptional regulations provided by the Act 4/1981 of 1 June on the states of alarm, emergency and siege (LSAES), during a state of emergency (which may be requested because of a serious alteration of essential public services), the government may intercept any type of communications provided that this is necessary to clarify alleged criminal offences or to maintain public order under Article 18 of the LSAES. The authorisation of the Congress in favour of a declaration of a state of emergency by the government must include the suspension of Article 18.3 of the Constitution, related to the secrecy of communication, in order for Article 18 of the LSAES to be applicable.

In addition, according to page 9 of the *Resolución modificación título habilitante 18032002*, relating to the telecommunications licence for the 1.800 MHz band, the licence owner must agree to:

i. whenever set out by the applicable laws, comply with the decisions issued by the authorities for the purposes of public interest, public safety and national security; and
ii. implement the necessary measures in order to be able to do this.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

As pointed out in the answer to Question 1 above, Article 43 of the LGTel enables the General Administration or a public body to request the encryption algorithms and procedures from, inter alia, any entity that includes an encryption mechanism within the services it provides.

However, the impact of this provision is rather low, due to the following considerations:

a. First of all, this provision was meant to lead to further development through complementary rules and regulations. Such development is still pending. For example, no additional specifications or definitions of the 'administrative or public body' entitled to request the algorithms have been produced yet. The effectiveness of this provision is doubtful, to say the least.

The situation may change if the government approves further developments. However, note that the first General Telecommunications Act of 1998 and the second General Telecommunications Act of 2003 contained similar provisions to the one discussed above. Neither such provisions have been developed through complementary regulations, and consequently, as far as we know, they were never applied. It is likely that no further development will occur any time soon.

b. The prerogative described above would only cover the algorithms and procedures used to encrypt the content and encryption devices for their control. It appears that there is no direct obligation to disclose information contained by a specific communication.

Notwithstanding this, the operator would still have to provide the judge, the Public Prosecutor or the agents of the judicial police with the necessary – albeit in this case, limited – assistance and collaboration to enable the fulfilment of legal interception orders, as stated in Article 588 ter e of the SCPA.

As the enablement of end-to-end encryption would compromise the telecommunications operator's ability to comply with its existing legal obligations in the area of law enforcement assistance, it is questionable whether this would raise issues with the government or the regulator. There is no legal precedent in this regard.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

To our knowledge, there are no such examples of 'old law' being used in order to demand access to data protected through encryption.

Tanzania

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

The Electronic and Postal Communication Act

The Electronic and Postal Communication Act of 2010 (the **EPOCA**) does not specifically make provision for the interception of customer communications. However, the existence of intercept powers can be implied from Section 120 of the EPOCA which states that no person without lawful authority under the EPOCA or any other written law can intercept, attempt to intercept or procure any other person to intercept or attempt to intercept any communications. An application must be made under 'any other law' to the director of public prosecution (the DPP) for authorisation to intercept or listen to any customer communication transmitted or received. Only public officers or an officer appointed by the Telecommunications Regulatory Authority (the TCRA) and authorised by the Ministry of Science and Technology and the Ministry of Home Affairs may be permitted to intercept such communications.

Section 120 of the EPOCA states that any person commits an offence, who, without lawful authority under the EPOCA or any other written law, does any of the following:

a. intercepts, attempts to intercept or procures any other person to intercept or attempt to intercept any communications;
b. discloses, or attempts to disclose to any other person the contents of any communications, knowingly or having reason to believe that the information was obtained through the interception of any communications in contravention of this Section; or
c. uses or attempts to use the contents of any communications, knowingly or having reason to believe that the information was obtained through the interception of any communications in contravention of this Section.

This Section therefore implies that any person with lawful authority may intercept customer communications.

Tanzania Intelligence and Security Service Act

The Tanzania Intelligence and Security Service Act Cap 406 R.E. 2002 (the **TISSA**) states that the Tanzania Intelligence and Security Service (the Service) has a duty to collect by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain, information and intelligence in respect of activities that may on reasonable grounds be suspected of constituting a threat to the security of Tanzania or any part of it. Section 15 of the TISSA further states that the Service has the power to investigate any person or body of persons whom it considers, or which it has reasonable cause to consider, a risk or source of a risk of a threat to state security. The Service may conduct any investigations which are required to provide security assessments.

Section 10 of the TISSA allows the Director-General of the Service the command, control, direction, superintendence and management of the Service and all matters connected with it. However, all orders and instructions to the Service issued by the Director-General are subject to any orders issued by the President of the United Republic of Tanzania, unless the minister responsible for intelligence and security directs otherwise in writing.

Prevention of Terrorism Act

According to Section 31 of the Prevention of Terrorism Act of 2002 (the **PTA**), subject to obtaining prior written consent from the Attorney-General, a police officer may make an application, *ex parte*, to the court for an interception of communications order to obtain evidence of the committing of an offence of terrorism under the PTA. The court to which an application is made may make an order:

a. requiring 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; and
b. authorising the police officer to enter any premises and to install on those premises any device for the interception and retention of a specified communication of a specified description, and to remove and retain such device.

This can only be done if the court is satisfied that the written consent of the Attorney-General has been obtained and that there are reasonable grounds to believe that material information relating to a terrorism offence or the whereabouts of a person suspected by a police officer to have committed an offence is contained in a certain communication or communications.

Tanzania

Criminal Procedure Act

Section 10 of the Criminal Procedure Act Cap 20 R.E. 2002 (the **CPA**) provides or grants the powers to police officers to investigate the facts and circumstances of a case where they have reason to suspect the committing of an offence. Further, section 10(2) of the CPA specifically gives the police officers powers, by order in writing, to require any person (natural or legal) who from information given in any other way appears to be acquainted with the circumstances of a case, or who is in possession of a document or anything else relevant to the investigation of a case, to attend or to produce the document or other item.

2. Disclosure of communications data

The Electronic and Postal Communication Act

Section 91 of the EPOCA allows that a database be kept with the TCRA in which all subscriber information will be stored. Every application services licensee must submit a monthly list to the TCRA containing its subscribers' information.

Regulation 4(2)(b) of the Electronic and Postal Communication (Telecommunications Traffic Monitoring System) Regulations of 2013 (the **TTMS Regulations**) allows the TCRA to acquire, install, operate and maintain traffic monitoring and measurement devices at the operator's premises. Moreover, Regulation 8 of the TTMS Regulations allows, inter alia, the traffic monitoring system to collect call detail records without intercepting any of the contents of communications such as voice or SMS. Call detail records have been defined as information generated by telephone exchanges which contains details of calls originating from, terminating at or passing through the exchange.

In addition, Regulation 13(4) of the TTMS Regulations states that the TCRA must ensure that call detail records data are collected exclusively to monitor compliance with the TTMS Regulations; they must be encrypted and stored with the last three digits of the calling numbers hashed in order to protect confidentiality; and call detail records collected are not to be transmitted or given to third parties, public or private, except as permitted by law.

The EPOCA provides that information may only be disclosed by an authorised person where it is required by any law enforcement agency, court of law or other lawfully constituted tribunal authority with respect to subscriber information.

However, according to the Electronic and Postal Communications (Licensing) Regulations of 2011 (the **Licensing Regulations**), a licensee may collect and maintain information on individual consumers where it is reasonably required for its business purposes. It further provides that the collection and maintenance of information on individual consumers must be:

a. fairly and lawfully collected and processed;
b. processed for identified purposes;
c. accurate;
d. processed in accordance with the consumer's other rights;
e. protected against improper or accidental disclosure; and
f. not transferred to any party except as permitted by any terms and conditions agreed with the consumer, as permitted or approved by the Authority, or as permitted or required by other applicable laws or regulations.

Under Section 99 of the EPOCA, a person will not disclose any information received or obtained in exercising powers or performing duties in terms of the EPOCA except where the information is required by any law enforcement agency, court of law or other lawfully constituted tribunal.

Notwithstanding this, any authorised person who executes a directive or assists with its execution and obtains knowledge or information of any communication may:

i. disclose such information to another law officer to the extent that it is necessary for the proper performance of the official duties of either of them; or
ii. use such information to the extent that it is necessary for the proper performance of official duties.

3. National security and emergency powers

The National Security Act

The National Security Act Cap 47 R.E. 2002 (the **NSA**), which makes provisions relating to state security, states in Section 15 that where the DPP is satisfied that there are reasonable grounds for suspecting that an offence under the NSA has been or is about to be committed, and that some person may be able to provide information about it, he or she may, by writing under his or her hand, authorise a named officer to require that person to give a police officer any information he or she has relating to the suspected or anticipated offence.

Tanzania Intelligence and Security Service Act

Section 5 of the TISSA gives authority to the Service to obtain, correlate and evaluate intelligence relevant to security, and to communicate any such intelligence to the minister and to persons whom, and in the manner which, the Director-General considers it to be in the interests of security. In doing so, the Service will cooperate as far as practicable and necessary with other state organisations and public authorities within or outside Tanzania that are capable of assisting the Service in the performance of its functions.

Tanzania

Constitution of the United Republic of Tanzania

The Constitution of the United Republic of Tanzania of 1977 as amended from time to time (the Constitution) provides Parliament with the power to enact and enable measures to be taken during a state of emergency or in normal times in relation to persons who are believed to engage in activities which endanger or prejudice the security of the nation.

Article 31 of the Constitution provides that any law enacted by Parliament will not be void for the reason only that it enables measures that derogate from the right to life to be taken during a state of emergency or in normal times in relation to persons who are believed to engage in activities which endanger or prejudice the security of the nation.

4. Oversight of the use of powers

Other than as outlined above, there is no judicial oversight of these powers. However, Section 114 of the EPOCA states that the TCRA may take enforcement measures against any person who contravenes the licence conditions, regulations and provisions of the EPOCA.

Censorship-related powers

1. Shut-down of network and services

Electronic and Postal Communications (Licensing) Regulations of 2011

Regulation 36 of the Electronic and Postal Communications (Licensing) Regulations of 2011 empowers the Tanzania Telecommunications Regulatory Authority (TCRA) to cancel or revoke the licence of a telecommunications provider (such as Vodacom) where the terms and conditions of that licence have been breached. The TCRA must issue a written notice to the licensee 30 days prior to the revocation of the licence. Were the TCRA to revoke Vodacom's licence, Vodacom would not be able to provide any telecommunications services and, in effect, its network would shut down.

2. Blocking of URLs and IP addresses

Tanzania Communications Regulatory Authority Act of 2003

The TCRA may, in fulfilling its functions, require a network provider (such as Vodacom) to block certain websites if they contain obscene material (the term 'obscene material' is not defined in the Act). The TCRA may do so by issuing a compliance order on the network provider concerned according to Section 45 of the Tanzania Communications Regulatory Authority Act of 2003. A compliance order is enforceable as an order of the High Court.

3. Power to take control of Vodacom's network

Electronic and Postal Communication Act of 2010

The police or the TCRA have the power to take control of Vodacom's network but only in the limited circumstances set out in Section 163 of the Electronic and Postal Communication Act of 2010. Under Section 163, a police officer or employee authorised by the TCRA may seize network equipment where he or she has reasonable grounds to believe that the electronic communication system supported by that equipment contravenes the terms of the licence issued to it by the TCRA or is otherwise in breach of the 2010 Act (or any regulations made under the Act). If no prosecution follows a seizure, the network equipment can be re-claimed within two months of the date of seizure or it is deemed forfeited.

4. Oversight of the use of powers

Electronic and Postal Communications (Licensing) Regulations of 2011

There is no judicial review of the TCRA's use of its powers under Regulation 36 of the Electronic and Postal Communications (Licensing) Regulations of 2011.

Tanzania Communications Regulatory Authority Act of 2003

There is no judicial review of the TCRA's use of its powers according to Section 45 of the Tanzania Communications Regulatory Authority Act of 2003.

Electronic and Postal Communication Act of 2010

Where a network provider's equipment is seized according to Section 163 of the Electronic and Postal Communication Act of 2010, it is possible for that network provider to seek the release of its equipment. When the network provider applies to the TCRA, the matter is referred to the Resident Magistrate's court or a district court by the TCRA who preside on the TCRA or police officer's action and decide whether the network equipment should be forfeited or released.

Tanzania

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

We are not aware of any express legal powers in this area. We would presume that the government would have the authority to require any network operator to decrypt communications data where it has applied the encryption – but only to the extent that such decryption was necessary for the law enforcement assistance (see 'Provision of real-time lawful interception assistance' and 'Disclosure of communications data' earlier in this chapter).

The most significant and relevant legal development has been the passing of the new Cybercrimes Act of 2015 (the **CA**), which may be applicable to this question. That said, the CA does not specifically seek to regulate encrypted material. However, Section 22(2), which creates the offence of obstruction of investigation sets out the following:

A person who intentionally and unlawfully prevents the execution or fails to comply with an order issued under this Act, commits an offence and is liable, on conviction, to a fine of not less than three million shillings or to imprisonment for a term of not less than one year or to both. [own emphasis]

It is clear from this provision that a service provider may become criminally liable if it fails to adhere to an order made according to the CA.

In particular, when looking at the law enforcement assistance orders concerning 'search and seizure' as set out in Part IV of the CA, the CA (among other things):

a. provides the ability to compel disclosure of data derived from being in the service provider's possession or control; and

b. states that the data disclosure must be in a form that is legible and can be taken away.

Points (a) and (b) appear to be highly relevant to the issue of decryption and would suggest that a communications service provider could be required to decrypt data that is within its possession or control in order to make such data legible to the party serving the order.

To our knowledge, there has been no matter before the Tanzanian courts that has tested the precise reach of this provision. In our view, however, the provision seems capable of being applied to compel a service provider to decrypt data in the circumstances set out above.

In respect of the disclosure and collection of traffic data where there are reasonable grounds that a computer system is required for the purpose of investigation, the provisions are extensive. They allow orders to be made by the police or the court for the disclosure, collection or recording of the traffic data associated with a specified communication during a specified period. They also permit and assist the law enforcement officer to collect or record that data. It is our view here that these provisions may extend to the issue of compelling decryption.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

The key issue here is the extent that the encrypted data is in the service provider's possession or control.

This, in our view, would have to be determined by the relevant body or court. If there is only a remote chance of the telecommunications operator being able to decrypt the data because the data in question has been encrypted by a third party, then this may nullify issues of whether the service provider is in possession or control.

The CA does not appear to compel a service provider to go to any lengths regarding the data that passes through its network and this is clear, for example, in Part V of the Act, which deals with liability of service providers. There are no monitoring obligations, for example. However, it is noteworthy that:

The Minister may prescribe procedures for service providers to:

a. *inform the competent authority of alleged illegal activities undertaken or information provided by recipients of their service; and*

b. *avail competent authorities, at their request, with information enabling the identification of recipients of their service.*

With regard to whether a telecommunications operator would be required to provide equipment interference or other forms of assistance, it appears that the CA has the potential to be able to proscribe such a procedure. Bearing in mind the provisions set out in the National Security Act (NSA) and the Tanzania Intelligence Security Services Act (TISSA), there appear to be a number of avenues available to the Tanzanian authorities to be able to compel the telecommunications operator to decrypt data – even to the extent of providing some form of 'equipment interference' if the telecommunications operator was determined to be a source of risk threatening national security following Section 15 of the TISSA. The TISSA also provides the ability to enact specific regulations that would enable the Service to carry out its duties under the Act.

Tanzania

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

The law does not specifically refer to end-to-end encryption. It is our view that if certain services are out of scope to the telecommunications operator, then the data cannot properly be said to be in the telecommunications operator's possession or control. See also the answer to Question 2 above.

That said, because the telecommunications operator may be perceived as having deliberately enabled a technology that puts its customers' data out of the telecommunications operator's possession or control, and therefore prevents the telecommunications operator from complying with its existing law enforcement assistance obligations as described earlier in this chapter, the telecommunications operator providing access to and/or facilitating such a service might be deemed controversial.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

We have not come across any 'old law' apart from the Constitution, the NSA and the TISSA, which in their original forms predated 1990 and the advent of commercial encryption.

However, the legal powers referred to earlier in this chapter (eg the legal powers under the Constitution, the NSA, the TISSA and the Emergency Powers Act) are broad where national security issues are at stake. In this context, therefore, it is not farfetched to conceive of a situation where specific legislation would be enacted to compel the telecommunications operator to decrypt data, and/or to put in place whatever it could, to assist the authorities if, for example, this was deemed necessary to thwart a perceived real national security risk.

In our view, such conduct would be open to the Tanzanian authorities, notwithstanding the possibility of this being challenged by judicial review in certain circumstances.

Turkey

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Note that Law No. 6698, the Personal Data Protection Law, was passed by the Parliament on 24 March 2016 and published in the *Official Gazette* on 7 April 2016. The Law is enforceable from the publication date. Guidance and details of its implementation are being worked upon; the Code itself envisages a six-month transition period for harmonisation and compliance. Twelve months after the enforcement date, secondary legislation will be published. The Law outlines a relatively similar framework to the European data protection system, although further changes are necessary if Turkish legislation is to completely align with the European Union's data protection regime. Article 51 of the Electronic Communications Law has entitled the Information and Communication Technologies Authority to govern the processing of personal data and protection of privacy in the electronic communications sector.

Real-time interception and disclosure powers

1. Provision of real-time lawful interception assistance

The Turkish Constitution

Article 22 of the Turkish Constitution states that interception of communication will be granted if *there is a decision duly given by a judge on one or several of the grounds of national security, public order, prevention of crime, protection of public health and public morals, protection of the rights and freedoms of others; or in non-delayable cases if there exists a written order of an agency authorised by law, again on the abovementioned grounds.*

'Agencies authorised by law' means any governmental body that is established pursuant to their establishment rules. Examples of agencies authorised by law or intelligence bodies are: the director general of public security, the commander of the Turkish gendarmerie forces (at their duty stations) and the director of intelligence agency.

The 'law' here can either be a Law, a Decree-Law or a Regulation which is below the Decree-Law in the hierarchy of laws, according to the Turkish legal system. The agency authorised by law includes the Information and Communication Technologies Authority (the BTK), establishment of which is required by the Law of Electronic Communications No. 5809 (*5809 Sayılı Elektronik Haberleşme Kanunu*). Unfortunately, 'non-delayable cases' are defined not within the Constitution but only in a variety of Regulations (eg the Regulation on Forensic Prevention (of Crimes) and Search and the Regulation on Seizure, Arrest and Interrogation). In general, as mentioned in the Regulation on Forensic Prevention (of Crimes) and Search, non-delayable cases include:

a. judicial reasons such as *the risk of disappearing of tracks, traces, marks and evidence of a crime, escaping of a suspect or disability of identification in case of not taking necessary action immediately; and the fact of not being able to obtain a verdict of the judge by reason of inadequate time to prevent the said risks;* and

b. prevention of crime when a condition is *jeopardising the protection of or causing the breach of national security and public safety, general health and public moral or the rights and liberties of others, disability of locating any illegally carried or possessed weapons or materials* because of not being able to obtain a verdict from the judge in adequate time to prevent those risks. However, the Court of Appeal may widen the scope of this definition depending on each case, so it remains open to potentially wide interpretation.

The Regulation on Authorisation within the Electronic Communication Sector, published in the *Official Gazette* No. 27241 and enforceable since 27 May 2009 (*Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği*) (the Regulation)

Article 21 of the Regulation empowers the BTK to intercept (or suspend, interrupt or stop) electronic communications operators from providing a communications service (entirely or partially), if the 'legal conditions of protecting the public safety, public health, public morals and other public interests as such' are met. If these conditions are met, the BTK will obtain the opinion of the Transportation and Communication Ministry in order to decide on the interception of communications provided by the relevant operator(s).

For the purposes of the Regulation, 'interception' may also mean suspension, interruption, stopping and/or blocking.

Note that according to the hierarchy of the governmental bodies, the BTK is bound to the Ministry of Transportation and Communication; hence the Ministry's opinion will be taken where necessary. 'Where necessary' is an ambiguous expression because there are no absolute grounds or occasions that are objectively necessary for the Ministry's opinion.

Turkey

The Regulation on the Procedures Organising the Publications on the Internet, published in the *Official Gazette* No. 26716 and enforceable since on 30 November 2007 (*Internet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik*) (the Internet Regulation)

As for communications made via the internet, Article 12 of the Internet Regulation states that, as a general rule, if there is 'adequate doubt' that publishing constitutes 'promoting suicide', 'sexual harassment of children', 'expediting usage of drugs', 'providing material harmful for health', 'obscenity', 'prostitution', 'providing venues and opportunities for gambling' and 'crimes against Ataturk' (the founder and the first president of the Republic of Turkey), access to that publishing will be intercepted and/or blocked. This decision can be given as a protection measure by the judge or, in non-delayable cases, by the prosecutor to submit for the judge's decision within 24 hours and then the judge will approve or abolish it within 24 hours. This article is in line with Article 8/1 of Law No. 5651 on the Regulation of Internet Publications and Prevention of Crime.

The same Regulation (Article 14) includes an 'administrative measure' and states that the Presidency of Telecom Communications (the TIB) may decide to intercept or block access to the relevant content on the grounds of 'promoting suicide', 'sexual harassment of children', 'expediting usage of drugs', 'providing material harmful for health', 'obscenity', 'prostitution', 'providing venues and opportunities for gambling' and 'crimes against Ataturk' (the founder and the first president of the Republic of Turkey) *ex officio*, if the content provider or the hosting service provider is located or residing abroad.

The orders of the TIB are sent directly to the internet access providers, including operators who provide access to the internet. The TIB may also decide to intercept or block access whether or not the content or the hosting provider is located or residing abroad, if the internet publishing constitutes 'sexual harassment of children' or 'obscenity', provided that its decision is submitted before the judge and the verdict on it is given within 24 hours. Article 16 of the Regulation states that access providers will set up the necessary hardware and software, and make the required arrangements in order to enable the immediate application of the access-blocking decisions via a connection between the TIB and the access provider.

While the BTK has its own administrative and financial autonomy, as mentioned in Article 4 of the Regulation for the Organisation of the BTK, the TIB is bound directly to the president of the BTK and serves within the BTK, according to Article 16 of the Regulation for Detecting, Recording and Wire-Tapping the Communications, and Evaluating the Signal Data, published in the *Official Gazette* No. 25989 on 10 November 2005 (*Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi Ve Kayda Alınmasına Dair Usul Ve Esaslar İle Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev Ve Yetkileri Hakkinda Yönetmelik*).

According to Article 16 of the Internet Regulation, the order of the TIB is sent to the internet access providers, including operators, via electronic means and will be applied by the access providers within 24 hours of the delivery of the order. However, this order will be subject to legal examination.

The Regulation for the Organisation of the BTK, published on a Decree of Council of Ministers numbered 2011/1688 and dated 4 April 2011, published in the *Official Gazette* No. 27958 and enforceable since 8.11.2011 (*Bilgi Teknolojileri ve İletişim Kurumu Teşkilat Yönetmeliği* – the Organisation Regulation)

Article 5/(u) of the Organisation Regulation states that any and all types of information can be obtained by the BTK from operator enterprises, state institutions, real persons and legal entities and, if requested by the Ministry, the BTK will deliver the information deemed necessary for determining sector-specific strategies and policies[1] to the Ministry. Therefore, operators are obliged to provide the necessary information on the BTK's request. Here 'any and all types of information' is a rather broad term and may include the documents and/or information relating to technical requirements for interception. In Article 5/(ü) of the Organisation Regulation, the BTK is entitled to take all precautionary actions stated by law so that the activities within the sector are carried out according to the requirements of national security, public order or public services.

Further to this, Article 5/1 of The Regulation on Authorisation within the Electronic Communication Sector, published in the *Official Gazette* No. 27241 and enforceable since 27 May 2009 (*Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği*) states that the Transportation Ministry's strategy and policies will be taken into account while the operators establish the technical infrastructure when authorised by the BTK. 'Strategy and policies of the Ministry' is another broad term which may conceivably be used by the Ministry to increase the flexibility of its actions within the communications sector.

1. Regarding the 'sector-specific strategies and policies', the Ministry publishes 'strategic plans' applicable for some specific years, ie 2014–2018, which may include, for instance, 'Establishing Data Systems for Electronic Communication Infrastructures (EHABS), carrying infrastructure data to electronic media, determining policies for the establishment of 4th generation communication infrastructures' and so on. The Turkish official text of the strategic plan for 2014–2018 can be accessed via: http://www.ubak.gov.tr/BLSM_WIYS/UBAK/tr/dokuman_ust_menu/stratejikplan/20090612_170301_204_1_64.pdf

Turkey

Intelligence authorities and legal enforcement authorities (agencies authorised by law) have the technical and technological capabilities to access an operator's systems. Therefore, a written order of the agencies authorised by law, including the BTK or a decision of a judge, is adequate for them to implement interception capabilities.

The Regulation for Detecting, Recording and Wire-Tapping the Communications and Evaluating the Signal Data, published in the *Official Gazette* No. 25989 on 10 November 2005 (*Telekomünikasyon Yoluyla Yapilan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi Ve Kayda Alinmasina Dair Usul Ve Esaslar İle Telekomünikasyon İletişim Başkanliğinin Kuruluş, Görev Ve Yetkileri Hakkinda Yönetmelik*) (the Wire-Tapping Regulation)

The Wire-Tapping Regulation is important because activities such as 'wire-tapping' mean accessing the content of telecommunications and require a high threshold. The Wire-Tapping Regulation gives wire-tapping powers to the intelligence bodies, such as the Security General Directorate or Intelligence Head or Gendarmerie General Command, by delivering their written order to the relevant offices for appropriate execution. These orders can be given in urgent cases for prosecution of specific sorts of crimes such as organised drug trafficking, organised economic crimes, sedition, crimes against the constitutional unity, national security and governmental confidentiality and espionage.

In a case where there is 'serious danger' against the essential interests of the country and the democratic constitutional state, and if the case is deemed to be 'urgent', written orders may be given to grant the security of the government, reveal espionage (spying activities), ascertain disclosure of state secrets and prevent terrorist activities. These orders would be given by the secretary and/or deputy secretary of the National Intelligence Organisation, and delivered to the relevant offices for appropriate execution (Article 7).

The 'relevant offices', where the written orders will be sent, appear to be those of the TIB. According to Article 10 of the Wire-Tapping Regulation, written orders and decisions will be sent to the TIB via the electronic means determined by the TIB. The orders and decisions are then applied under the TIB's supervision. The date and time of the activity and the identity of the person who conducted the activity will be determined and recorded by a written report. Orders which do not comply with the rules set by the Wire-Tapping Regulation will not be applied or enforced in any case.

2. Disclosure of communications data

Law No. 5651 on the Regulation of Internet Publications and Prevention of Crime

Before the Constitutional Court's decision of 2 October 2014, numbered 2014/149 E 2014/151 K, which was given only eight months after the publication of Article 3/4 of Law No. 5651 on the Regulation of Internet Publications and Prevention of Crime, internet access providers were obliged to provide communications data requested by the TIB, including:

- a subscriber's name;
- identity information;
- the address;
- the phone number;
- the date and time of logging into a system;
- the date and time of logging off a system;
- the IP address given for the relevant access and access points, and/or resource IP address and port number;
- the targeted IP address and port number;
- the protocol type;
- the URL address;
- the date and time of connection; and
- the date and time of ending of the connection.

This data could only be obtained by the TIB where a court order was given in relation to the prosecution of a crime. However, this sentence in Article 3 (namely, Article 3/4) was cancelled and retroactively abolished by the decision of the Constitutional Court due to a breach of the Constitutional 'principle of clarity and definiteness' stated in Article 2 of the Turkish Constitution and due to a breach of Article 20 of the Constitution which determines the core of personal data protection in Turkey. Following the cancellation, internet access providers are now obliged to provide this data if requested by the courts.

The TIB's and BTK's actions may be brought before the administrative courts for cancellation.

As for the content of the communications, such data falls within the scope of personal data definition in the new Personal Data Protection Law No. 6698 ('the **new DP Law**'). Although some Articles of this new DP Law will enter into force on 7 October 2016 (ie six months after the publication date), most protection clauses are already in force. According to the new DP Law, the 'data controller' will determine the purposes/objectives and instruments/manners of data processing and will establish and administer a data recording system. However, the obligation for data controllers to register with the 'data controller's registry' will enter into force on 7 October 2016.

Turkey

Considering that Vodafone deals not only with communications data, but also with other personal data, such as the customer's ID number and other ID details such as location, phone number, etc, this Law may prevail on most cases. After the relevant Articles enter into force, transferring of personal data to third parties, either within or outside the Turkish Republic, will be subject to the explicit consent of the data owner (Article 8 of the DP Law), as a general rule. The most striking exceptions to this rule include the conditions when transferring of data is:

- *mandatory in order to be able to use/ grant/protect a right;*
- *necessary provided that transferring of that data directly related with reaching or performing of an agreement; and*
- *mandatory for the data controller to fulfil a legal obligation.*

The content of communications cannot be accessed by the BTK or the TIB according to the Electronic Communication Sector legislation. However, if in a particular case pending before the prosecutor, the prosecution or the criminal procedure requires it, then the content may be disclosed to those administrations. This rule is also in line with the above-mentioned Articles of the new DP Law.

On 27 March 2015, the Electronic Communications Law Article 51/10-C introduced a change to the mandatory data retention period for communication data, according to which, the data retention period is reformulated to a maximum of two years and a minimum of one year.

3. National security and emergency powers

The Turkish Constitution

Intelligence authorities and agencies authorised by law (including the BTK) have the power to intercept communications for national security, public order, prevention of crime, protection of public health and public morals, and protection of the rights and freedoms of others. Therefore, they are entitled to take all necessary actions relating to these reasons, as detailed in Article 22 of the Constitution.

According to Article 15 of the Constitution and Law No. 2935 enacted on 25 October 1983 on State of Emergency, communications may be intercepted permanently, or the tools to provide communications to customers may temporarily be seized for reasons of public emergency, national security, mobilisation or war.

In applying Law No. 2935, a declaration of extraordinary administration procedures may be the result of a natural disaster or a serious economic crisis, widespread acts of violence or serious deterioration of the public order. The right to communicate and the privacy of communications and personal life may be restricted entirely or partially, which could hand the control of all authorisations mentioned above to the entities indicated in the decree laws.

The Council of Ministers, under the chairpersonship of the President of the Republic and after consultation with the National Security Council, may declare martial law in one or 60 more regions throughout the country for a period of no more than six months in the event of:

- widespread acts of violence which are aimed at the destruction of the free democratic order or the fundamental rights and freedoms embodied in the Constitution and more dangerous than the cases requiring a state of emergency;
- war;
- the emergence of a situation requiring war;
- an uprising;
- the spread of strong and violent and rebellious actions against the motherland and the Republic; or
- widespread acts of violence of internal or external origin threatening the indivisibility of the country and the nation.

4. Judicial and official oversight

Under Article 22 of the Turkish Constitution, an authorised agency's order (apart from that of the BTK) will be submitted for a judge's approval within 24 hours. The judge's decision will be declared in the 48 hours following the submission; otherwise the order of the authorised agency will be abolished *per se*.

The Turkish legal system is based on the continental European legal system. In this respect, the actions, orders and decisions of a governmental body can be subject to cancellation or nullity claims before the administrative courts and not the civil courts.

Administrative courts cannot act on behalf of the administrative bodies, but merely implement precautionary suspensions of administrative actions and then decide on either the cancellation or nullity, or approval, of such actions. In that sense, the BTK's decision and/or Transportation and Communication Ministry's opinion are not subject to judicial oversight, unless they are brought before administrative courts for cancellation.

Although other authorised agencies' orders, eg a prosecutor's order in an urgent case, must be approved by a judge, it appears the BTK's actions of interception of communication services are not subject to a

Turkey

judge's prior approval. However, they can still be subject to litigation before administrative courts for their validity and enforceability.

According to Article 17 of the Internet Regulation, if the prosecutor decides there is no adequate evidence to create suspicion (an 'adequate suspicion' threshold) then the order will be abolished *per se*. In urgent cases during the prosecution process, however, the prosecutors themselves may decide to intercept or block the content. This decision must be brought before the judge within 24 hours and the judge will decide on the matter within 24 hours. Unfortunately, what amounts to an urgent case is not defined within the Internet Regulation, so it remains quite open to interpretation.

Article 8 of the Wire-Tapping Regulation states that an authorised agency's order, such as an order of the Security General Directorate or Intelligence head, the Gendarmerie General Command or the Secretary of the National Intelligence Organisation, will be submitted to a judge's approval within 24 hours. The judge's decision will be declared in the 48 hours following the submission; otherwise the order of the authorised agency is abolished per se.

The decision for conducting wire-tapping or other interception measures can be given for a period of three months at most. This period can be extended up to three times making a maximum period of nine months (ie 3 x 3 = 9).

The decision of the intelligence bodies (Security General Directorate, Gendarmerie General Command or National Security Organization) or the prosecutor must be approved by the judge in the 24 hours following their submission, or the order will be abolished.

Censorship-related powers

1. Shut-down of network and services

A network operator, such as Vodafone, must obtain authorisation of the Communication Technologies Authority (the BTK) to legally operate its network.

The Regulation on Information and Communication Technologies Authority Administrative Penalties published in the *Official Gazette* No. 28914 and enforceable since 15 February 2014 (*Bilgi Teknolojileri Ve İletişim Kurumu İdari Yaptirimlar Yönetmeliği*)

In cases of war, mobilisation and/or public emergency, the BTK may order the shut-down of all or some of a network operator's (such as Vodafone's) services for a limited or indefinite period of time if requested to do so by government agencies responsible for public security and national defence. This is stated in Article 34 of the Regulation on Information and Communication Technologies Authority Administrative Penalties. Given the broad nature of such powers, it is feasible that they might extend to ordering the shut-down of Vodafone's entire network. If a network operator did not comply with such an order, this non-compliance would constitute gross negligence and the operator's authorisation to provide network services would be terminated.

The BTK can also terminate authorisation entirely where a network operator (such as Vodafone) breaches national security or public order rules under Articles 31 and 32 of the Regulation on Information and Communication Technologies Authority Administrative Penalties.

Electronic Communications Law

Network operators must comply with the procedures and proceedings in the Electronic Communications Law; this includes obtaining the BTK's authorisation in order to legally operate as a network operator. The procedure for obtaining authorisation is set out in detail in Article 9. The BTK has the power to suspend or revoke authorisation to operate a network if the operator in question contravenes its obligations under the Electronic Communications Law or if the BTK considers the operator to have been grossly negligent in operating its network or services.

2. Blocking of URLs and IP addresses

Law No. 5651 on the Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publications

Article 9 of Law No. 5651 obliges network operators (such as Vodafone) to take all technological measures to prevent access to IP addresses or URLs which are marked as providing access to illegal content by a court decision or by the Presidency of Telecom Communications Head Office (the TIB). The Union of Access Providers (established 19 May 2014) is responsible for notifying operators of a court or TIB decision; network operators are then obliged to carry out the necessary blocking within four hours of receiving such notice.

A new omnibus law published recently provides the Chairman of the TIB with the power to request the blocking of websites and content in order to protect national security and public order, as well as to prevent crime. Upon receiving such a request, the service provider is required to shut down the website or remove the content specified within four hours.

In the past year, the Constitutional Court has annulled Article 4/3, Article 5/5 and Article 6/1/(d) of Law No. 5651, which obliged content providers, hosting service providers

Turkey

and access providers to share all the data kept by them with the TIB, in the manner requested by the TIB. These articles were found to be in breach of the Constitutional 'principle of clarity and definiteness' stated in Article 2 of the Constitution and of Article 20 on the protection of private life and personal data. The Constitutional Court also annulled an expression in Article 9/9 which stated that 'a decision of a judge regarding a publication that breached a personal right' will also apply to 'identically similar publications'. In this article, the expression of 'identically similar publications' was annulled by the Constitutional Court on the grounds that it breached 'freedom of thought' in Article 26 of the Constitution and the rule of 'limiting the fundamental rights only by Laws' (and not hierarchically lower regulations) in Article 13 of the Constitution.

According to these changes, access providers can no longer be forced to block IP addresses which are similar to the IP addresses blocked previously. The Constitutional Court's decision is enforced one year after publication in the *Official Gazette*. As the publication date was 28 January 2016, the changes are expected to be enforced one year after publication in the *Official Gazette*. The Court's decision was published on 28 January 2016.

3. Power to take control of Vodafone's network

The Regulation on Information and Communication Technologies Authority Administrative Penalties

See Section 1 'Shut-down of network and services' above. In cases of war, mobilisation and/or public emergency, the BTK may take control of Vodafone's network according to Article 34 of the Regulation on Information and Communication Technologies Authority Administrative Penalties. The BTK must have a written order from the government agencies responsible for public security and national defence to do so.

4. Oversight of the use of powers

The BTK's decisions are administrative acts and subject to legal procedures. Therefore, a relevant party (eg in the circumstances described above, a network operator such as Vodafone) could commence a lawsuit to cancel a decision taken by the BTK before the relevant legal authorities.

Where the Chairman of the TIB requests the blocking of a website or removal of certain content, that request is submitted to the Criminal Court of Peace for approval by a judge within 24 hours. The judge must then decide whether to approve the request within 48 hours.

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes. Turkish legislations do not directly mention any obligation for communications service providers (CSPs) to decrypt communications. However, the tools, infrastructure and any requirement for decrypting the data must be provided to the agencies authorised by law or intelligence bodies (eg the BTK or the TIB) when they require them in order to detect, wire-tap and record the communications under the legal conditions set out earlier in this chapter (see 'Provision of real-time lawful interception assistance').

In particular, the TIB is entitled to make CSPs establish and provide the necessary infrastructures, tools and means that enable wire-tapping, detecting and recording of communication (Regulation for Detecting, Recording and Wire-Tapping the Communications Article17/1/(e)).

Also, the TIB's Department for Information System is entitled to integrate some mechanisms to decrypt the communications or order the integration of them, if and when an encrypted communication is detected during a wire-tapping mission. In the case of a CSP not complying with the obligation to provide necessary infrastructure to the TIB, administrative fines (eg up to 3% of the net sales profit of the previous calendar year) will apply.

Also, the BTK is entitled to inspect and control the CSPs to see whether they apply the technical requirements provided by laws and regulations, as stated in the Electronic Communications Law No. 5809 (Article 59). In order for the BTK to duly perform this 'inspection', it may request from the operators 'any and all kinds of information' which is a broad definition and may well include encrypted data. However, in theory, the content of the communication cannot be examined by the BTK but only by the agencies authorised by law or intelligence bodies.

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

Even in cases where the communication data is encrypted by third parties, the above-mentioned rules will apply.

Turkey

The legislation does not directly mention any obligation for CSPs to decrypt communication. However, the TIB's Department of Information Systems can integrate or order to integrate necessary mechanisms in the system in order to decrypt the communication, according to Article 21/A of the Regulation for Detecting, Recording and Wire-Tapping of Communications. The same rule applies when a CSP does not produce the encryption system itself, but merely provides the infrastructure for third parties' use of its network, as in an OTT service provider's services. In such cases, decryption would be performed by the TIB not the CSP itself.

Hence, a judge's verdict or, in non-delayable cases, an order of prosecutors (if the investigation has already started) or agencies authorised by law or intelligence bodies (if the aim is prevention of crime), will be enforced by the TIB's Head of Information Systems Department. To do this, the Head can request that a telecommunications operator integrates the necessary systems accordingly, in order to let the Department decrypt the communication. Without that specific request, the telecommunications operator is not obliged to interfere with the communication to decrypt it. The decryption will be handled by the Department. All communications data will be held by the Department for 10 days at most, and destroyed after 10 days (Article11 of Regulation for Detecting, Recording and Wire-Tapping of Communications).

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

Turkish legislation and applications only cover, at least at the present time, the conditions when traditional encrypted communications systems are produced and applied by the CSPs themselves.

However, legislation does include a permission rule if the entity can be accepted as a 'producer of encrypted communication device/systems' according to the 'Regulation on Principle and Procedures for Coded or Encrypted Communications of Public Entities and Real or Legal Persons'. Therefore, depending on the technical details of the encrypted communications services that a telecommunications operator conducts, the operator may have to apply to the BTK for a permit to produce the end-to-end encryption system.

This subject is relatively new for the BTK, because the laws were drafted when encrypted communications were only possible via devices that provided encryption; eg encrypted mobiles and transmitters. Accordingly, no practical approach of the BTK may be foreseen or indicated at the time of writing. However, the BTK may have to examine and decide whether or not such an encryption system needs official permission. In order to avoid any possible illegal conduct, the operator may use its 'right to obtain information' by explaining some technical details of the system, if not all, and obtain an official writ thereon, which may also be an example for future applications.

If the BTK requires official permission to start end-to-end encryption activities, the telecommunications operator must apply with:

- documents of the encryption technique/device and technical specifications of the electronic communication to be used;
- the encryption algorithm;
- modules for producing, distributing and uploading the encryption key, and the software or hardware which decrypts the code/encrypted data if necessary;
- optional software/hardware, tools and other apparatus which will be used during a test if necessary;
- a signed circular of authorised real/legal persons; and
- the content of the technical document as stated in Annex 2 of the 1999/5/EC Regulation for Transmitters and Telecommunications Terminal Equipment (applicable since 24 March 2007).

Permission of the BTK must also be secured for any kind of alterations or updates to be made to the encryption system (Articles 5 and 7 of the Regulation on Principles and Procedures for Coded or Encrypted Communications of Public Entities and Real or Legal Persons).

Whoever makes or provides encrypted communication without complying with these rules will face a judicial monetary sentence of 500 to 1,000 days (ie from 10,000 to 100,000 TL), as well as administrative fines up to 3% of net sales profit of the previous calendar year, according to Article 10 of the Regulation and to Articles 60 and 63 of the Electronic Communications Law No. 5809.

This Regulation also shows that the CSPs must only provide the BTK with some technical information, instead of decrypting the encrypted communications data themselves.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

The legislation applied prior to the above-mentioned Regulation on Principle and Procedures for Coded or Encrypted Communications of Public Entities and Real or Legal Persons was called the 'Regulation on Encrypted Transmitter Systems', the latest version of which was dated 6 March 2004 and was published in the *Official Gazette* No. 25394. However, this Regulation was entirely

Turkey

abolished by the new Regulation. The other relevant previous legislation was the 'Transmitter Law' No. 2813 which was entirely abolished after the articles of the Electronic Communications Law No. 5809 entered into force.

In Turkey, unless a concrete case occurred on a date that the previous (abolished) legislation was in force, the abolished law cannot be applied whatsoever and it cannot override the current legislation. As with criminal legislations, if a case occurred on a date when the abolished legislation was applicable, the legislation which is more beneficial for the suspect or the accused will apply.

Note that this 'beneficial code' principle only applies to criminal matters and not civil ones. For instance, in a decision given by the Court of Appeal's General Assembly of Civil Chambers dated 2 April 2014 and numbered 2013/13-661 E 2014/440 K, the abolition of the Transmitter Law was determined and the Articles of the new Electronic Communications Law were found applicable. Another example is the criminal case, which was decided by the 7th Circle of Criminal Chamber of the Court of Appeal, dated 1 January 2014 and numbered 2012/25235 E 2014/341 K. In this case, the Court of Appeal stated that the Transmitter Law was entirely abolished by the new Electronic Communications Law after the date of the alleged crime, but it also ordered the Criminal Court to examine the 'beneficial law' principle for the alleged criminal.

Although these cases do not include encrypted communication matters, they indicate that previous laws cannot override new laws, but that in some cases beneficial law may apply.

UK

In this report, we provide an overview of some of the legal powers government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers, as well as some of the legal powers government agencies have to restrict our network and services or block URLs or IP addresses. We also provide an analysis of the laws related to encryption in the context of law enforcement assistance.

This content was updated following analysis that was conducted in spring 2016.

Real-time interception and disclosure powers

1. Provision of real-time interception assistance

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (**RIPA**) gives senior cabinet ministers the power to authorise the interception of a person's communications following an application made by an intelligence or law enforcement agency (LEA).

Under Section 5 of RIPA, any Secretary of State can issue an intercept warrant where he or she believes:

- it is necessary in the interests of national security for the purpose of preventing or detecting serious crime or for the purpose of safeguarding the economic wellbeing of the UK; and
- that the conduct authorised by the warrant is proportionate to its intended purpose.

An interception warrant must name or describe either one person as the interception subject or a single set of premises as the premises in relation to which the relevant interception is to take place (Section 8(1) of RIPA).

However, under Section 8(4)(b) of RIPA, the relevant Secretary of State has broader authority in relation to external communications. He or she may issue a certificate accompanying an interception warrant relating to external communications that provides for the interception of material that he or she considers it is necessary to examine. RIPA defines the term 'external communication' as a communication sent or received outside the British Isles (Section 20 of RIPA). The Interception of Communications Code of Practice (**IOC COP**) states that an external communication does not include communications both sent and received in the British Isles, even if they pass outside the British Isles (page 22 of IOC COP).

Section 11(4) of RIPA establishes a general requirement on public telecommunications service providers in the UK to take all reasonably practical steps requested by the relevant LEA to give effect to an interception warrant.

In addition to the general requirement to assist in giving effect to a warrant under Section 11(4), the Secretary of State may, under Section 12 of RIPA, order a public telecommunications service provider to maintain an interception capability. Under Section 12 of RIPA and the Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002 (SI 2002/1931), the relevant Secretary of State has the authority to order a public telecommunications service provider to maintain the practical capability to assist in relation to intercept warrants. To carry out the order, a notice is given in accordance with the order to the relevant service provider. The powers in question only apply to providers of a public telecommunications service whose service is intended to be provided to more than 10,000 people.

Intelligence Services Act 1994

Under Section 5 of the Intelligence Services Act 1994 (**ISA**), the Secretary of State may, on an application made by the Security Service, the Intelligence Services or GCHQ, issue a warrant in respect of any specified property or in respect of wireless telegraphy. This power may be broad enough to permit the government direct access to Vodafone's network by the Security Services in some instances. Although large parts of ISA have been repealed, Section 5 is still in force.

A warrant under Section 5 of the ISA will be granted by the Secretary of State if he or she is satisfied that:

- the taking of the action by the Security Service, the Intelligence Service or GCHQ is necessary to assist the particular agency in carrying out any of its statutory functions;
- it is necessary and proportionate to what the agency seeks to achieve and could not reasonably be achieved by other (less intrusive) means; and
- satisfactory arrangements are in place to ensure that the agency will not obtain or disclose information except insofar as necessary for the proper discharge of one of its functions.

Section 11(1)(a) of RIPA provides for the possibility that an intercept warrant can be effected by the LEA or intelligence agency that applied for it without any assistance. One interpretation of this is that in instances where interception takes place via a pre-existing intercept capability, the LEA or intelligence agency need not inform the service provider in question that the intercept has occurred.

UK

2. Disclosure of communications data

Regulation of Investigatory Powers Act 2000

RIPA gives LEAs, intelligence agencies and a wide range of other public authorities the legal authority to acquire metadata relating to customer communications. The powers require anyone who provides a telecommunications service to disclose customers' metadata they possess or are able to obtain. The powers relate to traffic data, service use information and subscriber information, but not the content of the communications.

Under Section 22(4) of RIPA, a notice may be issued by a person holding a prescribed office, rank or position within a relevant public authority designated with the power to acquire communications data by order under Section 25(2) and under the Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010/480).

Under Section 22(3) of RIPA, persons within a public authority may be given an authorisation to directly obtain the communications data in question in certain circumstances, for example where notification may prejudice an investigation or operation.

Under Section 22(2) of RIPA, the designated person can only issue a notice or an authorisation where they believe it is necessary on one of eight grounds. These include:

- in the interests of national security;
- to prevent or detect crime or prevent disorder;
- in the interests of the economic wellbeing of the UK; and
- in the interests of protecting public safety or to protect public health.

The designated person must believe that the conduct authorised by the notice or authorisation is proportionate.

3. National security and emergency powers

Telecommunications Act 1984

Under Section 94 of the Telecommunications Act 1984 (**Section 94**) and after consultation with OFCOM and/or providers of public electronic communications networks, the Secretary of State may give OFCOM or the network provider general directions as he or she believes necessary in the interests of national security or relations with the government of a country or territory outside the UK. Although the Communications Act 2003 superseded most of the Telecommunications Act 1984, Section 94 is still in force.

Under Section 94, if network providers are given directions to do or not do something as directed by the Secretary of State, they must not disclose them if the Secretary of State has notified them that he or she believes that disclosure is against the interests of national security or relations with the government of a country or territory outside the UK. The Secretary of State may, with the approval of the Treasury, make grants to providers of public electronic communications networks to defray or contribute towards any losses the network provider may sustain by reason of compliance with the directions under Section 94.

Communications Act 2003

Under Section 132 of the Communications Act 2003, the Secretary of State may require OFCOM, the UK's communications regulator, to give a direction to suspend or restrict the network, services or facilities of an electronic communications network provider or an electronic communications service provider to protect the public from any threat to public safety, to public health or in the interests of national security.

Civil Contingencies Act 2004

Under the Civil Contingencies Act 2004 (**CCA**), the government is given broad powers for a limited period of time during civil emergencies. These include the authority to protect or restore systems of communications such as Vodafone's network. The government's emergency powers could, in theory, extend to other actions in relation to Vodafone's network.

As an operator of a public electronic communications network that makes telephone services available (whether for spoken communication or for the transmission of data), Vodafone would be classified as a Category 2 Utility Responder under the CCA (Schedule 1 Part 3 of the CCA).

Under Sections 1 and 19 of the CCA, disruption to a system of communication may constitute an emergency for the purposes of Part 1 of the Act. Part 1 addresses local arrangements for civil protection. Part 2 addresses emergency powers.

Under Section 6(1) of the CCA, the government may require or permit Vodafone to disclose information on request to another organisation or person designated as an emergency responder under the CCA in connection with their functions in the emergency.

Under Sections 20 and 22 of the CCA, the Queen or senior Cabinet ministers (in practice the Home Secretary) may make emergency regulations for protecting or restoring a system of communication if they are satisfied that this is appropriate for preventing, controlling or mitigating an aspect or effect of the emergency in question.

UK

4. Oversight of the use of powers

The judiciary plays no role in the authorisation of interception warrants under RIPA. The Interception of Communications Commissioner, appointed under Section 57(1) of RIPA, keeps under review the exercise and performance of the interception powers granted under RIPA. These include the power of the Secretaries of State to issue intercept warrants and the procedures of the agencies involved in conducting interception. The Commissioner presents an annual report to the Prime Minister which is published on the website of the Interception of Communications Commissioner's Office.

The Investigatory Powers Tribunal, established under Section 65 of RIPA, hears complaints in relation to powers granted under RIPA. It is also the only forum that hears complaints about any alleged conduct by or on behalf of the British intelligence agencies (MI5, MI6 and GCHQ). It may award compensation, quash intercept warrants or authorisations and order the destruction of any records obtained by an intercept warrant or authorisation. The decisions of the Tribunal are not subject to appeal or questioning by any court in the UK. A decision by the Tribunal not to uphold a claim based on the Human Rights Act 1998 could be taken to the European Court of Human Rights in Strasbourg if certain conditions of that Court were satisfied.

If a public telecommunications service provider believes that a Section 12 of RIPA notice places unreasonable technical and/or financial demands on it, it may refer the issue to a specialist panel of advisors that is set up under Section 13 of RIPA called the Technical Advisory Board (TAB). The TAB reports its conclusions to the relevant Secretary of State, who may either withdraw the notice or issue a new notice. Note that the Section 12 order and notice procedure is outside the remit of the Interception of Communications Commissioner (Section 57(2)(a) of RIPA).

Regarding the disclosure of communications data, under Section 37 of the Protection of Freedoms Act 2012 and Sections 23A and 23B of RIPA, local authorities are required to gain judicial approval from a local magistrate for an authorisation or notice to acquire communications data. There is no judicial oversight in relation to the approval of notices or authorisations issued by law enforcement agencies or intelligence agencies.

The judiciary plays no role in the authorisation of interception warrants under Section 5 of ISA. The Intelligence Services Commissioner, appointed under Section 59(1) of RIPA, keeps under review the exercise and performance of the powers granted by Section 5 of ISA. The Commissioner presents an annual report to the Prime Minister, who lays it before the Houses of Parliament. It is published on the Commissioner's Office website.

There is governmental oversight in relation to the directions given under Section 94, as the Secretary of State must lay a copy of every direction given before each House of Parliament, unless he or she believes that disclosure of the direction is against:

- the interests of national security;
- relations with the government of a country or territory outside the UK; or
- the commercial interests of some other person.

The CCA sets limits on the emergency regulations that can be made under it (Section 23 of CCA). For example, any emergency regulations must be laid before, and approved by, Parliament as soon as practicable after first being made (Section 26(1)(a)). In any event, they automatically lapse after 30 days (Section 27). Emergency regulations may not amend the Human Rights Act 1998 (Section 23(5)(a)). The Houses of Parliament may pass resolutions cancelling the emergency regulations or amending them (Section 27).

Censorship-related powers

1. Shut-down of network and services

Communications Act 2003

Under Section 132 of the Communications Act 2003, the Secretary of State may require OFCOM, the UK's communications regulator, to give a direction to suspend or restrict the network, services or facilities of an electronic communications network provider or an electronic communications service provider to protect the public from any threat to public safety, to public health or in the interests of national security.

2. Blocking of URLs and IP addresses

Terrorism Act 2006

Although the government does not have the legal authority to require Vodafone to block IP addresses, a process exists under Section 3 of the Terrorism Act 2006 which allows a police constable to require the removal or modification of terrorism-related material. This provision is designed to apply to the providers of hosting services, rather

UK

than those carrying communications and, as such, it is unlikely to apply to Vodafone's electronic communications network or the provision of electronic communications services.

Where a police constable believes illegal terrorism-related material is available on a website, he or she may serve notice on the person(s) responsible for that material, requiring the material's removal or modification within two working days. According to official guidance on notices issued under Section 3, such notices can be served on anyone involved in the provision or use of electronic services, including the content provider, hosting internet service providers (except where they are acting as 'mere conduits') and webmaster. Therefore, Vodafone could be required by the police to remove or modify illegal terrorism-related material where Vodafone hosts that content. In respect of its network, Vodafone is likely to be considered a 'mere conduit'.

If a person fails to comply with a notice served under Section 3, he or she will not be able to use the defence of non-endorsement contained in Sections 1 and 2 of the Terrorism Act 2006 should prosecution ensue under those Sections. Therefore, if Vodafone did not comply with a police notice, it would potentially incur criminal liability.

3. Power to take control of Vodafone's network

Civil Contingencies Act 2004

Under the CCA, the government is given broad powers for a limited time during civil emergencies. These include the authority to protect or restore systems of communications such as Vodafone's network. The government's emergency powers could, in theory, extend to other actions in relation to Vodafone's network. Part 1 of the CCA addresses local arrangements for civil protection; Part 2 addresses emergency powers.

An emergency is defined in Sections 1 and 19 as:

- an event or situation which threatens serious damage to human welfare in a place in the UK;
- serious damage to the environment of a place in the UK; or
- war, or terrorism, which threatens serious damage to the security of the UK.

Disruption to a system of communication (eg a mobile network) may constitute an emergency for these purposes.

MTPAS

The Mobile Telecommunication Privileged Access Scheme (MTPAS) is an agreed protocol between network operators and the police. MTPAS is designed to address the issue that, when a major emergency incident occurs, mobile networks tend to experience abnormally high concentrations of calls jeopardising the network itself (since the network may not be able to cope with such high volumes of traffic). MTPAS ensures that those providing support to the scene of the emergency incident (such as police and ambulance services) are able to continue using the network.

Under MTPAS, when a major emergency incident occurs, the Police Gold Commander in charge of responding to that incident can notify network operators (including Vodafone) that a major incident has occurred. A provider would then take steps to ensure that the mobile network continues to operate and does not break down under the increased volumes of traffic made by ordinary network users in response to the incident. Individuals with privileged access to the network consist of Category 1 and 2 Responders (as defined in the CCA) and partner organisations directly supporting them at the scene of the incident.

4. Oversight of the use of powers

Communications Act 2003

Where a provider of a public electronic communications network or service receives a direction under Section 132 of the Communications Act 2003, that provider may appeal that direction to the Competition Appeals Tribunal.

More broadly, a provider may have the right to seek a judicial review of the Secretary of State's direction to Ofcom.

Terrorism Act 2006

Part 1 of the Terrorism Act 2006 (including Section 3) is subject to annual review by the Independent Review of Terrorism Legislation. The role of the Independent Reviewer of Terrorism Legislation is to inform the public and political debate on anti-terrorism law in the UK, in particular through regular reports which are prepared for the Home Secretary or Treasury and then laid before Parliament.

Civil Contingencies Act 2004

The CCA sets limits on the emergency regulations that can be made under it. For example, under Section 27, any emergency regulations must be laid before, and approved by, Parliament as soon as practicable after first being made and Parliament may pass resolutions amending or cancelling those emergency regulations. Section 23 states that emergency regulations may not amend the Human Rights Act 1998. Emergency regulations automatically lapse after 30 days according to Section 26.

UK

Encryption and law enforcement assistance

1. Does the government have the legal authority to require a telecommunications operator to decrypt communications data where the encryption in question has been applied by that operator and the operator holds the key?

Yes. Under Part I of the Regulation of Investigatory Powers Act 2000 (RIPA), the government has the power to impose a specific obligation to maintain intercept capability in relation to communications data. This relates to intercepted communications and the more general authority on disclosure of protected or encrypted electronic data (including communications data) under Part III of RIPA.

i. Section 12 of RIPA: Maintenance of intercept capability

Under Section 12 of RIPA and the Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002 (SI 2002/1931) (see 'Provision of real-time interception assistance' above), the relevant Secretary of State has the authority to order a public telecommunications service provider to maintain the practical capability to assist in relation to intercept warrants. The order can be carried out by giving a notice in accordance with the order to the relevant service provider.

Paragraph 10 of Part II of the Schedule to the 2002 Order is an obligation on the service provider to 'ensure that the person on whose application the interception warrant was issued is able to remove any electronic protection applied *by the service provider* to the intercepted communication and the related communications data' [emphasis added].

ii. Part III of RIPA: Disclosure of protected or encrypted data

Part III of RIPA sets out the powers under which public authorities or other persons with the appropriate permission may ask persons to disclose protected or encrypted data. Under Section 49(2) of RIPA, a notice requiring disclosure must be served on the person whom it is believed has possession of the code, password or algorithm required to access the protected information. Schedule 2 of RIPA sets out who has the appropriate permission to ask for the disclosure: the police, the National Crime Agency, HMRC and other persons holding office under the Crown.

A Section 49 notice can only be issued if the requirement of disclosure is proportionate to what is sought to be achieved and if it is not reasonably practicable to obtain the protected data in an intelligible form in any other way. In addition, the notice to disclose may only be served:

- in the interests of national security;
- for the purposes of preventing or detecting crime;
- in the interests of the economic wellbeing of the UK; or
- for the purposes of securing the effective exercise or proper performance by a public authority of any statutory power or statutory duty.

When a Section 49 notice is served on a person, he or she is entitled to use any key or password in his or her possession to obtain access to the protected data and disclose the information in an intelligible form, or, alternatively, to disclose the key itself (Section 50(1) and (2)). A person who knowingly fails to make the disclosure required to satisfy the notice is guilty of an offence, punishable by imprisonment or a fine, or both.

The Investigation of Protected Electronic Information Code of Practice states that the National Technical Assistance Centre (NTAC) at Government Communication Headquarters must approve any Section 49 notice before permission is sought for that notice to be served. (However, since the Code of Practice is not binding, NTAC approval is not mandatory.) NTAC is the lead national authority for all matters relating to the processing of protected data into intelligible form.

In terms of judicial oversight, because protected data can be obtained in such a variety of scenarios, the rules on whether judicial approval is required to issue the relevant Section 49 notice are complex. In general terms, a Circuit judge (in England and Wales) can grant written authorisation to a public authority to serve the Section 49 notice. However, sometimes higher judicial approval is required; in other instances, no judicial approval is required. For example, where the protected data is obtained under an intercept warrant, then the Secretary of State who issued the warrant may give permission to issue the Section 49 notice.

Finally, because protected data may be acquired by a range of intelligence agencies, law enforcement agencies and public authorities acting under different parts of RIPA, the exercise of powers under Part III is also kept under review by the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Chief Surveillance Commissioner.

UK

2. Does the government have the legal authority to require a telecommunications operator to decrypt data carried across its networks (as part of a telecommunications service or otherwise) where the encryption has been applied by a third party?

We answer this question in two parts:

a. *Could a relevant state law enforcement body, intelligence agency or other authorised public body use Part III of RIPA as the legal basis for requiring a telecommunications operator to decrypt data encrypted by third parties?*

The current scope of the obligations in RIPA on CSPs in relation to the decryption of encrypted data carried over their networks is set out in our answer to Question 1 above. Public disclosures in recent months during the pre-legislative scrutiny of the Investigatory Powers Bill suggest that the Home Office interprets the decryption obligations in Part III of RIPA to apply to encryption applied by the CSP, not by third parties.

b. *What potential does a telecommunications operator have to be required to provide equipment interference or some other form of assistance in order to decrypt data encrypted by third parties?*

In certain circumstances, the Intelligence Agencies (the Security Service, the Secret Intelligence Service and GCHQ) and some law enforcement authorities appear to be able to authorise assistance from the telecommunications operator in order to facilitate the implementation of equipment interference powers. However, there is no indication that such powers could be used to oblige a telecommunications operator to decrypt third-party data.

Property and equipment interference powers are set out in:

- the Intelligence Services Act 1994 (**ISA**) in relation to the Intelligence Agencies; and
- the Police Act 1997 (the **PA**).

To answer the question, we will focus on the equipment interference powers (EI) available to the Intelligence Agencies under ISA.

The EI powers were publicly avowed in detail for the first time in February 2015 when the Home Office published a consultation on a draft Equipment Interference Code of Practice, on the same day that the Investigatory Powers Tribunal (IPT) published its second judgment in the action brought by Liberty, Privacy International and others.

During the course of 2015, more information about the statutory basis and operational use of EI powers was placed in the public domain, notably in the Intelligence and Security Committee's 'Report on Privacy and Security' published in March 2015 where details of GCHQ's activity known as Computer Network Exploitation (CNE) were set out. Submissions by Home Office personnel to the Parliamentary committees reviewing the Investigatory Powers Bill (the **IP Bill**) since November 2015 have also clarified to some extent the scope of the EI powers under ISA. The IPT judgment in the claim by Privacy International and seven ISPs, dated 12 February 2016, also further clarified the operational scope and statutory basis of CNE.

The Equipment Interference Code of Practice (the **EICOP**) was finally published in January 2016.

While the focus of this Legal Annexe is in relation to the current legal arrangements under ISA and RIPA, not what is proposed in the revised IP Bill, we note that ISA will not be repealed when the IP Bill becomes law, so the EI-related provisions of ISA will remain relevant in the context of the new Investigatory Powers Act in due course.

The EI powers are set out in Sections 5 and 7 of the ISA, with supplementary detail as to process in Section 6. Broadly speaking, Section 5 gives the Secretary of State authority to issue warrants authorising entry into or interference with property or wireless telegraphy in the UK if such action is likely to be of substantial value in assisting the Intelligence Agencies to fulfil their statutory functions. (This is subject to certain requirements including the usual statutory tests and purposes relating to investigatory powers.)

Section 7 provides the Secretary of State with a similar power of authorisation in relation to entry and interference outside the UK. Crucially, any such entry or interference authorised under Section 5 or Section 7 is not unlawful in the UK. This excludes actions from criminal and civil liability, notably under the Computer Misuse Act 1990.

The power to issue a warrant authorising interference contained in Section 5 of the ISA is couched in quite broad terms, and refers to 'assisting', as follows:

'authorising the taking ... of such action ... in respect of any property so specified or in respect of wireless telegraphy so specified if the Secretary of State ... thinks it necessary for the action to be taken on the ground that it is likely to be of substantial value in *assisting*, as the case may be ... the Intelligence Agencies' [emphasis added].

This wording does not appear to confine the scope of a warrant to authorising only actions undertaken by an Intelligence Agency. The wording of the EICOP underscores this interpretation. It states that property and equipment interference warrants under Section 5 of ISA and authorisations under Section 7 of ISA can be sought not only in respect of members of the Intelligence Agencies, but also in respect of persons acting on their behalf or in their support.

Furthermore, the Home Office's Investigatory Powers Bill, Government Response to Pre-Legislative Scrutiny, published in March 2016, in describing how important the cooperation

UK

of CSPs is for the use of investigatory powers, states on page 39 that 'the assistance of CSPs may also be necessary in order to gain direct access to a suspect's device by using equipment interference powers'.

So, it seems reasonable to assume that the government interprets the EI powers in ISA to include the ability to authorise a CSP's assistance in implementing equipment interference. There is, however, no indication that such EI powers could also be used to require a CSP to decrypt any third-party data itself. To the best of our knowledge, such a practice has not been publicly avowed during the official disclosures relating to the Investigatory Powers Bill.

3. Can a telecommunications operator lawfully offer end-to-end encryption on its communications services when it cannot break that encryption and therefore could not supply a law enforcement agency with access to cleartext metadata and the content of the communication on receipt of a lawful demand?

Our understanding is that the current powers under RIPA relating to the decryption of protected data (explained in Question 1 above) would apply to a CSP where the CSP is in 'possession' of the 'key' (both broadly defined in Part III of RIPA) that enables access to protected information.

On the face of it, the provisions of RIPA would not deter a CSP from offering a service that enables third parties to encrypt communications, so long as the CSP did not possess any key to such encryption.

However, to the best of our knowledge, the question of how the relevant provisions of RIPA could be interpreted as applying to the service provider of a service that was end-to-end encrypted (such that keys were only held on a customer's device) has not been specifically addressed in any publicly available court judgment or in the relevant Home Office Code of Practice.

As RIPA is drafted to be technology neutral, it applies in the same way to BAU and to OTT services.

Investigatory Powers Bill

We note that the question of whether the powers set out in the IP Bill could be used to compel a CSP to decrypt end-to-end encrypted data carried over the CSP's network has remained a prominent issue in the pre-legislative scrutiny phase of the IP Bill, focusing on the meaning of Clause 189 of the IP Bill (now Clause 217 of the revised Bill).

The Home Office's latest explanation of what is proposed is set out in Sections 6 and 7 of the revised draft EICOP (in relation to the anticipated Investigatory Powers Act) that was published on 1 March 2016, along with the revised IP Bill.

4. Please provide examples in your jurisdiction where legislation which predated the advent of commercial encryption (which we estimate to be circa 1990) has been applied to contemporary cases involving encryption.

There do not appear to be any such examples; in fact, in the recent case of *Laurie Love v National Crime Agency (NCA)*, the NCA applied to use 'old' legislation in this way and the court rejected its application.

The original seizure warrant was made under the Computer Misuse Act 1990. Mr Love applied for his seized hardware to be returned to him under the Police Property Act 1897 (**PPA**). Section 1 of the PPA allows an individual to make an application to the court for the return of an individual's property that is in the possession of the police.

In a hearing on 12 April 2016, the NCA sought a direction from the court that Mr Love provide his passwords in the interests of good case management, on the basis of the court's case management powers for civil proceedings under Rule 3A of the Magistrates' Court Rules 1981 SI 552 (as amended). The NCA further relied on the Criminal Procedure (Amendment) Rules 2016 SI 120 to attempt to persuade the court to order the disclosure of the encryption keys or passwords.

Mr Love submitted that the NCA should be making an approach under Section 49 of RIPA instead and that a court direction under its case management powers requiring the submission of the passwords in question would breach:

- Article 1 (respect of human rights);
- Article 8 (right to private and family life);
- Article 1 Protocol 1 rights (the right to property); and
- Section 3 of the Human Rights Act 1998.

The court agreed with Mr Love and rejected the NCA's application. In its judgment, the court stated at paragraph 10 that 'the case management powers of the court are not to be used to circumvent specific legislation that has been passed in order to deal with the disclosure sought', and that the correct approach would be to seek disclosure through the Section 49 procedure under RIPA.

On 10 May 2016, the City of Westminster Magistrates' Court decided not to grant the NCA's application for disclosure of encryption passwords from the claimant, Mr Love, in relation to encrypted material on computer hardware previously seized from him.

The judgment to the case is accessible here: https://www.judiciary.gov.uk/wp-content/uploads/2016/05/love-v-nca.pdf