Parliamentary Joint Committee on Intelligence and Security

Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

SUBMISSION
Vodafone Hutchison Australia

January 2015

Vodafone Hutchison Australia Pty Limited (VHA) makes this short submission to the Parliamentary Joint Committee on Intelligence and Security Inquiry into Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Data Retention Bill). We look forward to expanding on this paper in our appearance before the Comittee.

As well as participating in consultations with Government agencies, VHA has worked closely with the telecommunications industry's peak industry bodies, Communications Alliance (CA) and the Australian Mobile Telecommunications Association (AMTA), to assess the Data Retention Bill. We endorse the CA/AMTA submission and the recommendations contained within it. We note the following comment in the CA/AMTA submission, which is a useful summary of VHA's perspective:

> *The CSP sector has previously expressed its view, for example in submissions and testimony to the PJCIS in 2013, that it did not believe the Agencies, Attorney-General's Department nor Government had yet made a sustainable case for the imposition of a mandatory data retention regime in Australia. One significant consideration highlighted at that time was the potentially enormous cost impost on CSPs – and therefore, ultimately, Australian consumers. This view has not changed.*[1]

International comparisons

Australia has a robust, comparatively transparent law enforcement regime that includes a range of appropriate protections and formal requirements for access to customer information. As Parliament looks to make changes to the data retention requirements of the current regime it is vital that Australia continues to maintain high standards.

In June 2014 Vodafone Group released its inaugural international Law Enforcement Disclosure Report that provided a country-by-country analysis of law enforcement requirements. We believe that the Committee with find the international information useful in their considerations and therefore we attach the Disclosure Report for the Committee's information.

The importance of customer privacy and the need for protections in a national law enforcement regime

All telecommunications customers have a right to privacy. This right is enshrined in Australian privacy law and protecting this right is one of VHA's highest priorities. The privacy of our customers is also integral to the Code of Conduct and Privacy Policy which all employees must comply with at all times.

As a telecommunications operator in Australia, VHA is also required by law to assist Australian national security and law enforcement agencies. This may include disclosing customer information upon lawful request by an agency. The ability for certain agencies to be able request information from telecommunications companies is designed for the purposes of protecting national security and preventing or investigating crime. Requests may also be made by emergency services agencies in responding to emergency calls and life threatening situations.

[1] CA/AMTA, Submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) – Review of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, December 2014, page 2.

Importantly, there are a range safeguards and controls for all disclosures made to agencies in response to lawful requests. Vodafone will only comply with requests for customer information that are made in accordance with the law and there are strict governance controls within Vodafone to deal with each of these requests.

It is appropriate that as technology changes that the tools law enforcement agencies are adapted. In the process of changing the requirements it is important that the public gets a clear understanding of how the needs of both the consumers right to privacy and the citizen's right to live in a secure and safe nation are optimised. We agree with the recommendations of the PJCIS in its 2013 "Report of the Inquiry into Potential Reforms of Australia's National Security" if a metadata regime is to be put in place that there needs to be:

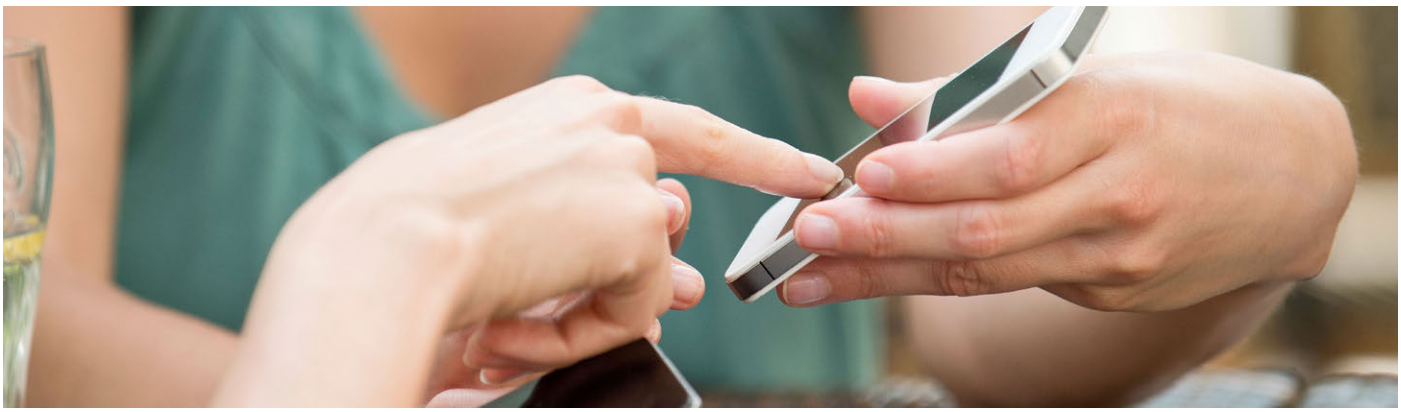
- clear protections for the privacy of communications
- proportionate but up to date investigative capabilities
- robust oversight and accountability.

The CA/AMTA submission provides detail on our perspectives on the overall legislative proposal. We would like to make some additional comments on the length of time the legislation is requiring to store metadata, most notably the proposal in regards to IP identifiers.

Data storage of IP-identifiers

The Government is proposing to require telcos to retain two-years of information about customers' 'metadata'. The Attorney General has flagged that this would include data storage of customer IP identifiers when an individual accesses the internet. While the IP-identifier is analogous to a traditional telephone number, there are differences. We believe that these differences warrant a period shorter for the data storage of IP identifiers:

- Two years is at the upper bound of the storage requirements being contemplated in Europe for this information. We note that the European Commission's Evaluation report on the Data Retention Directive, April 2011, which found that most data requested by enforcement agencies was less than six months old. This is consistent with our Australian experience.
- We also believe (and have received feedback from our customers) that IP-identifier data is substantially more sensitive information than traditional telephone call records.
- Generally, different IP-identifier numbers are allocated each time a customer accesses the internet or sends an online message and so each time a customer accesses the internet. It is our assessment of is that it will take some years to firmly establish a standard industry capability to store this data. In particular, before we introduced the capability we would need to be confident that we could protect every customer's privacy.



Law Enforcement Disclosure report

Our customers have a right to privacy which is enshrined in international human rights law and standards and enacted through national laws. Respecting that right is one of our highest priorities: it is integral to the Vodafone Code of Conduct which everyone who works for us has to follow at all times.

However, in every country in which we operate, we have to abide by the laws of those countries which require us to disclose information about our customers to law enforcement agencies or other government authorities, or to block or restrict access to certain services. Those laws are designed to protect national security and public safety or to prevent or investigate crime and terrorism, and the agencies and authorities that invoke those laws insist that the information demanded from communications operators such as Vodafone is essential to their work.

Refusal to comply with a country's laws is not an option. If we do not comply with a lawful demand for assistance, governments can remove our licence to operate, preventing us from providing services to our customers. Our employees who live and work in the country concerned may also be at risk of criminal sanctions, including imprisonment. We therefore have to balance our responsibility to respect our customers' right to privacy against our legal obligation to respond to the authorities' lawful demands as well as our duty of care to our employees, recognising throughout our broader responsibilities as a corporate citizen to protect the public and prevent harm.

Complex, controversial – and constantly changing

Communications technologies have evolved rapidly over the last 20 years. Almost three billion people[1] now communicate and share information over electronic communications networks on a regular basis, and vast volumes of data are created and exchanged every second. However, many of the legal powers relied upon by law enforcement agencies, intelligence agencies and other government authorities were first drafted in a much simpler era, when a household shared a single telephone landline, mobile phones were relatively rare and the internet as we understand it today did not exist. Our views on the legislative challenge in many countries are set out later in this report.

The use of those legal powers in the context of today's far more complex electronic communications has proven to be highly controversial. All governments have incorporated national security exceptions into national legislation to give legal powers to agencies and authorities. Some governments have constrained those powers to limit the human rights impact; others have created much wider-ranging powers with substantially greater human rights impacts. Meanwhile, agencies and authorities have the scope to apply advanced analytics techniques to every aspect of an individual's communications, movements, interests and associations – to the extent that such activity is lawful – yielding a depth of real-time insights into private lives unimaginable two decades ago.

In a number of countries, these changes have created tensions between the protection of the citizen's right to privacy and the duty of the state to ensure public safety and security. Those tensions have been heightened as a consequence of the allegations made by the former US National Security Agency (NSA) contractor Edward Snowden. Media reports of widespread government surveillance and data 'harvesting' by intelligence agencies have triggered a significant public debate about the transparency, proportionality and legitimacy – even lawfulness – of the alleged activities of a number of high-profile agencies.

Questions have also been asked about the role of communications operators such as Vodafone in support of those activities. We hope that this report will provide some of the most important answers, although there will undoubtedly be some questions that we cannot answer for reasons that we explain later in this report.

What we are publishing, and why

This is our inaugural Law Enforcement Disclosure report. We are also one of the first communications operators in the world to provide a country-by-country analysis of law enforcement demands received based on data gathered from local licensed communications operators. We will update the information disclosed in this report annually. We also expect the contents and focus to evolve over time and would welcome stakeholders' suggestions as to how they should do so.

Privacy and security – Law Enforcement Disclosure report

The report encompasses all 29 operating businesses directly controlled by Vodafone (including our joint ventures in Australia, Kenya and Fiji), in which we have received a lawful demand for assistance from a law enforcement agency or government authority between 1 April 2013 and 31 March 2014. We have not included countries in which we operate where no such demands were received, nor have we included countries where there may be some form of Vodafone brand presence (for example, through a partner market relationship) but where Vodafone does not own or control a licensed communications operator.

We have focused on the two categories of law enforcement demands which account for the overwhelming majority of all such activity: lawful interception; and, access to communications data. Both of these terms are explained later in this report. We have not included statistical data on the number of orders received to block or restrict access to content or services (further details of which are addressed below). We are exploring options to include this information in future reports, although it is important to note that there are complexities involved in collating the information required (content filters can be applied at various points within a country's various networks, some of which may not be visible to Vodafone) and a number of countries are likely to prohibit publication of this information.

The report is intended to:

- explain the principles, policies and processes we follow when responding to demands from agencies and authorities that we are required to assist with their law enforcement and intelligence-gathering activities;
- explain the nature of some of the most important legal powers invoked by agencies and authorities in our countries of operation;
- disclose the aggregate number of demands we received over the last year in each of our countries of operation unless prohibited from doing so or unless a government or other public body already discloses such information (an approach we explain later in this report); and
- cite the relevant legislation which prevents us from publishing this information in certain countries.

Compiling this report has been a very complex and challenging endeavour. Given the sensitivity of any discussion of agency or authority activity in certain countries, it has also not been without risk. We set out to create a single disclosure report covering 29 countries on a coherent basis. However, after months of detailed analysis, it has become clear that there is, in fact, very little coherence and consistency in law and agency and authority practice, even between neighbouring EU Member States. There are also highly divergent views between governments on the most appropriate response to public demands for greater transparency, and public attitudes in response to government surveillance allegations can also vary greatly from one country to another.

The transparency challenge

Law enforcement and national security legislation often includes stringent restrictions preventing operators from disclosing any information relating to agency and authority demands received, including disclosure of aggregate statistics. In many countries, operators are also prohibited from providing the public with any insight into the means by which those demands are implemented. These restrictions can make it very difficult for operators to respond to public demand for greater transparency. We provide further insight into the nature of those prohibitions later in this report.

We respect the law in each of the countries in which we operate. We go to significant lengths to understand those laws and to ensure that we interpret them correctly, including those that may be unpopular or out of step with prevailing public opinion but which nevertheless remain in force. In this report, we have therefore set out the laws and practices, on a country-by-country basis, that limit or prohibit disclosure. We believe this form of transparency is as important as the publication of aggregate demand statistics themselves in terms of ensuring greater public understanding in this area.

In a number of countries, the law governing disclosure is unclear. Under those circumstances, we have approached the authorities to seek clarity, wherever feasible. Some have given their assent to disclosure of aggregate statistical information about demands received. However, others have told us that we cannot publish this information. If we were to defy the responses received from the latter, we believe it is likely that our local businesses would face some form of sanction and that in some countries, individual Vodafone employees would be put at risk. Therefore, in our report this year we make no disclosure wherever the authorities have told us that we cannot do so. Similarly, where the authorities have not responded to our request for guidance or where the security situation means that any form of engagement with the authorities carries an unacceptable level of risk, we have not disclosed aggregate demand information out of concern for the safety of our employees. However, wherever possible, we will re-engage with the relevant authorities to seek updated guidance ahead of the publication of this report in future years. It is therefore possible that the level of disclosure permitted within the countries concerned may change over time as a result of that process.

Who should publish: governments or operators?

In our view, it is governments – not communications operators – who hold the primary duty to provide greater transparency on the number of agency and authority demands issued to operators. We believe this for two reasons.

First, no individual operator can provide a full picture of the extent of agency and authority demands across the country as a whole, nor will an operator understand the context of the investigations generating those demands. It is important to capture and disclose demands issued to all operators: however, based on our experience in compiling this report, we believe it is likely that a number of other local operators in some of our countries of operation would be unwilling or unable to commit to the kind of disclosures made by Vodafone in this report.

Privacy and security – Law Enforcement Disclosure report

Second, different operators are likely to have widely differing approaches to recording and reporting the same statistical information. Some operators may report the number of individual demands received, whereas others may report the cumulative number of targeted accounts, communications services, devices or subscribers (or a varying mixture of all four) for their own operations. Our views on the scope for considerable inconsistency in this area are explained later in this report. Similarly, multiple different legal powers may be invoked to gain access to a single customer's communications data: this could legitimately be recorded and disclosed as either multiple separate demands, or one.

To add to the potential for confusion, an agency or authority might issue the same demand to five different operators; each operator would record and disclose the demand it received in its own way (with all of the variations in interpretation explained below); and the cumulative number of all operators' disclosures would bear little resemblance to the fact of a single demand from one agency. Moreover, in countries where the law on disclosure is unclear, some operators may choose not to publish certain categories of demand information on the basis of that operator's appetite for legal risk, whereas another operator may take a different approach, leading to two very different data sets in the public domain.

Shortly before this report was published, other local operators in two of the countries in which we operate – Germany and Australia – began to publish their own law enforcement disclosure reports. Those reports included statistical information about some (but not all) types of agency and authority demands for assistance received by the operator in question. In both countries, the authorities also publish statistical information spanning all operators.

We have compared the statistical information we hold for our own operations in the two countries in question with the information recently published by other local operators in those countries. For some categories of agency and authority demand, the volumes involved seem closely comparable between Vodafone and other local operators, although as explained above, there is a significant risk of under or over-counting overlapping demands issued to multiple operators. Furthermore, it is also clear that certain categories of agency and authority demand have been omitted from local operators' publications, either to comply with legal restrictions (in the case of Australia) or (in Germany) for reasons not disclosed to us.

In our view, inconsistent publication of statistical information by individual operators amounts to an inadequate and unsustainable foundation for true transparency and public insight. There is a substantial risk that the combination of widely varying methodologies between operators (leading to effectively irreconcilable raw numbers) and the potential for selective withholding of certain categories of agency and authority demand (for reasons which may not themselves be fully transparent) would act as a significant barrier to the kind of meaningful disclosure sought by the public in an increasing number of countries.

We believe that regulators, parliaments or governments will always have a far more accurate view of the activities of agencies and authorities than any one operator. However, our belief is not without qualification. In order for publication of this statistical information by the authorities to be meaningful and reliable, in our view it must:

- be independently scrutinised, challenged and verified prior to publication;
- clearly explain the methodology used in recording and auditing the aggregate demand volumes disclosed;
- encompass all categories of demand, or, where this is not the case, clearly explain those categories which are excluded together with an explanation of the rationale supporting their exclusion; and
- encompass demands issued to all operators within the jurisdiction in question.

We believe governments should be encouraged and supported in seeking to adopt this approach consistently across our countries of operation. We have therefore provided links to all aggregate statistics currently published by governments in place of our own locally held information (where disclosure is legally permissible at all) and are already engaged in discussions with the authorities in a number of countries to enhance the level of transparency through government disclosure in future.

Separately, where the authorities currently do not publish aggregate statistical information but where we believe we can lawfully publish in our own right, we have disclosed the information we hold for our own local operations. In at least 10 of the 29 countries covered, the disclosures we make in this report represent the first time that this kind of information has been placed into the public domain by a locally licensed operator. However, our concerns about the inadequacy of this kind of disclosure remain. Wherever possible, we will therefore seek to work with other local operators to develop a consistent cross-industry recording and reporting methodology and will engage with governments to make the case for a central, independent and verified source of statistical information spanning all operators. We look forward to updating this report with the outcomes from those discussions.

Finally, we would emphasise that it is not possible to draw any meaningful conclusions from a comparison of one country's statistical information with that disclosed for another. Similar types and volumes of agency and authority demands will be disclosed (where public reporting is permitted at all) in radically different ways from one country to the next, depending on the methodology used. Similarly, changes in law, technology or agency or authority practice over time may make year-on-year trend data comparisons difficult in future reports.

Privacy and security – Law Enforcement Disclosure report

What statistics should be reported: warrants or targets?

In our country-by-country law enforcement disclosure section, we have focused on the number of warrants (or broadly equivalent legal mechanism) issued to our local businesses as we believe this is the most reliable and consistent measure of agency and authority activity currently available. The relatively small number of governments (9 out of the 29 countries covered in this report) that publish aggregate statistics also collate and disclose this information on the basis of warrants issued.

Each warrant can target any number of different subscribers. It can also target any number of different communications services used by each of those subscribers and – in a modern and complex all-IP environment – it can also target multiple devices used by each subscriber to access each communications service. Additionally, the same individual can be covered by multiple warrants: for example, more than one agency or authority may be investigating a particular individual. Furthermore, the legal framework in some countries requires agencies and authorities to obtain a new warrant for each target service or device, even if those services or devices are all used by the same individual of interest. Note that in the majority of countries, warrants have a time-limited lifespan beyond which they must either be renewed or allowed to lapse.

As people's digital lives grow more complex and the number of communications devices and services used at home and work on a daily basis continues to increase, the ratio of target devices and services accessed to warrants issued will continue to increase. To illustrate this with a hypothetical example:

- a single warrant targets five individuals;
- each individual subscribes to an average of eight different communications services provided by up to eight different companies: a landline phone line, a mobile phone, two email accounts, two social networking accounts and two 'cloud' storage accounts; and
- each individual owns, on average, two communications devices fitted with a SIM card (a smartphone and a tablet) in addition to a landline phone and a laptop.

In the hypothetical example above, that one warrant could therefore be recorded as more than 100 separate instances of agency and authority access to individual services on individual devices used by individual subscribers. The scope for miscounting is immense.

In our view, the most robust metric available is the number of times an agency or authority demand for assistance is *instigated* – in effect, a formal record of each occasion that the state has decided it is necessary to intrude into the private affairs of its citizens – not the extent to which those warranted activities then range across an ever-expanding multiplicity of devices, accounts and apps, access to each of which could be recorded and reported differently by each company (and indeed each agency or authority) involved.

We therefore believe that disclosure of the number of individual warrants served in a year is currently the least ambiguous and most meaningful statistic when seeking to ensure public transparency. However, over time it is possible that an alternative means of providing accurate and reliable aggregate statistical data will emerge as a result of our engagement with other operators and with governments in those countries where publication of this information is permitted.

Privacy and security – Law Enforcement Disclosure report

Security and secrecy: The limits on what local licensed operators can disclose

Beyond a small group of specialists, very few people understand the laws invoked by agencies and authorities when requiring a local licensed communications operator such as Vodafone to provide assistance. In part, that lack of understanding arises because those laws also impose strict secrecy obligations on those involved in the processes: the more you know, the less you are allowed to say.

Our decision to make the disclosures set out in this report is therefore not without risk. In some countries, providing what to many observers would seem to be relatively anodyne information about the legal powers and processes used by agencies and authorities could lead to criminal sanctions against Vodafone employees. The main restrictions on disclosure are set out below.

Obligations on individual employees managing agency and authority demands

In each of our operating companies around the world, a small number of employees are tasked with liaising with agencies and authorities in order to process demands received. Those employees are usually security-cleared to a high level and are bound by law to absolute secrecy. They are not permitted to discuss any aspect of a demand received with their line management or any other colleagues, nor can they reveal that a demand has been received at all, as doing so could potentially compromise an active criminal investigation or undermine measures to protect national security. Additionally, in some countries, they cannot even reveal that specific law enforcement assistance technical capabilities have been established within their companies. In many countries, breaching those restrictions would be a serious criminal offence potentially leading to imprisonment.

Furthermore, even the limited number of employees aware of a demand will have little or no knowledge of the background to, or intended purpose of, that demand. Similarly, the individual employees involved will not be aware of all aspects of the internal government approval process involved, nor will they know whether or not an agency or authority is cooperating with – or working on behalf of – an agency or authority from another jurisdiction when issuing a demand using Mutual Legal Assistance Treaty (MLAT) arrangements concluded between governments.

All such demands are processed 'blind' with no information whatsoever about the context. Whilst we can – and do – challenge demands that are not compliant with legal due process or seem disproportionate, it is therefore not possible for Vodafone to ascertain the intended purpose of any demand received. Equally, we cannot assess whether or not the information gathered as a result of a demand will be used in a manner which is lawful, nor, in most cases, can we make any judgement about the potential consequences of complying (or failing to comply) with an individual demand.

It is also important to note that in seeking to establish whether or not an individual has been involved in unlawful activity, agency and authority demands may encompass access to information regarding many other individuals who are not suspected of any crime. The confidentiality obligations imposed on operators are therefore also intended to prevent inadvertent disclosure of private information related to individuals who are not suspects but whose data may help further an investigation or prove that they are a victim.

Restrictions on disclosing technical and operational systems and processes

Many countries require communications operators such as Vodafone to comply with specific technical and operating requirements designed to enable access to customer data by agencies and authorities. There are wide-ranging legal restrictions prohibiting disclosure of any aspect of the technical and operating systems and processes used when complying with agency and authority demands. In some countries, it is unlawful even to reveal that such systems and processes exist at all.

The small number of Vodafone employees familiar with the systems and processes involved are prohibited from discussing details of these with line management or other colleagues, and the circulation within the company of general information related to those systems and processes is heavily restricted or classified.

Restrictions on disclosing details of the aggregate number of demands received

In some of our countries of operation, we are prohibited in law from disclosing aggregate statistics relating to the total number of demands received over a 12 month period. In others, the law may expressly prohibit the disclosure that law enforcement demands are issued at all. In a number of countries where the law on aggregate disclosure is unclear, the relevant authorities have told us that we must not publish any form of aggregate demand information. We believe that defying those instructions could lead to some form of sanction against our local business and – in some countries – would also present an unacceptable level of risk for individual employees, to whom Vodafone owes a duty of care.

Whilst we have included factors relevant to national security powers in compiling this report, it is important to note that many countries prohibit the publication of any form of statistical information relating to national security demands.

Further details can be found in the country-by-country law enforcement disclosure section.

How we work with law enforcement agencies and government authorities

At Vodafone, our customers' privacy is paramount. We have strict governance controls in place across all of our businesses worldwide to ensure the protection of our customers' data and communications. We are committed to following the UN Guiding Principles for Business and Human Rights. We are also a founding member of the Telecommunications Industry Dialogue on Freedom of Expression and Privacy (the Industry Dialogue'). The Industry Dialogue is a group of global communications operators who work together and in collaboration with the Global Network Initiative to address a range of human rights and privacy challenges. We are a signatory to the Industry Dialogue's Guiding Principles on Freedom of Expression and Privacy, which defines a common approach to be taken by operators when dealing with demands from governments, agencies or authorities that may affect our customers' privacy and freedom of expression. Further details of Vodafone's policies and principles in these areas can be found in the Privacy and security section of the sustainability report.

As we explain in our Privacy and law enforcement principles below, Vodafone is committed to meeting its obligations to respond to agencies' and authorities' lawful demands but will not go beyond what is mandated in law (other than under specific and limited circumstances, again outlined below).

Abiding by those principles can be challenging in certain countries at certain times. In practice, laws governing agencies' and authorities' access to customer data are often both broad and opaque, and – as explained below – frequently lag the development and use of communications technology. Furthermore, the powers in question are often used in the context of highly sensitive and contentious developments – for example, during major civil unrest or an election period – which means that Vodafone colleagues dealing with the authorities in the country in question can be put at risk for rejecting a demand on the basis that it is not fully compliant with the law.

We can – and do – refuse to comply with demands that are unlawful. The majority of rejections tend to be for defects in the legal process or documentation or in response to demands which appear to be issued under an inappropriate legal power. We do not yet have sufficiently robust reporting mechanisms to record all such refusals, so these are not listed in this report. We will consider how best to address this shortcoming where possible, in future reports.

Demands for assistance made by agencies or authorities acting beyond their jurisdiction will always be refused, in line with our principles. It is important to note that we have not, in fact, received any such cross-border demands. Were we ever to receive such a demand, in providing our refusal in response, we would inform the agency or authority that they should consider any MLAT processes to seek the cooperation of the relevant domestic agency or authority with the necessary lawful mandate.

As a general principle, our dealings with agencies and authorities fall into one of the three categories below. If we receive a demand for assistance which falls outside these three categories, we will challenge it and refuse to comply.

Mandatory compliance with lawful demands
We will provide assistance in response to a demand issued by an agency or authority with the appropriate lawful mandate and where the form and scope of the demand is compliant with the law. Each of our local operating businesses is advised by senior legal counsel with the appropriate experience to ensure compliance with both the law and with our own principles.

Emergency and non-routine assistance
Our policy allows for the provision of immediate emergency assistance to agencies and authorities on a voluntary basis where it is clear that it is overwhelmingly in the public interest for us to do so. These are very specific circumstances where there is an imminent threat to life or public safety but where existing legal processes do not enable agencies and authorities to react quickly enough. Common examples include a police request for assistance whilst a kidnapping is in progress or to locate a missing child.

Under these circumstances, we will respond immediately to a request for assistance so long as we are satisfied that the agency making the request has the legal authority to do so. We will then require the formal lawful demand to follow soon thereafter with retrospective effect. We are clear in our policy that discretionary assistance is granted on an exceptional basis and cannot be used by agencies and authorities as a routine alternative to compliance with legal due process. All such instances are scrutinised carefully under our governance rules.

Protecting our customers and our networks
We work with law enforcement agencies on a voluntary basis to seek to prevent or investigate criminal and hacker attacks against our networks and to prevent or investigate attempts to defraud our customers or steal from Vodafone. We also cooperate on a voluntary basis on broader matters of national infrastructure resilience and national security. We have similar arrangements with banks and our peers under which we share intelligence on how best to protect our customers and our businesses from illegal acts. We believe that this form of cooperation – which does not involve providing agencies with any access to customer data – is strongly in the interests of our customers and the public as a whole. It is important to note that this form of cooperation does not involve providing agencies and authorities with any access to customer data: moreover, we believe it is strongly in the interests of our customers and the public as a whole.

Privacy and security – Law Enforcement Disclosure report

The Vodafone privacy and law enforcement principles

We do not:

- allow any form of access to any customer data by any agency or authority unless we are legally obliged to do so;
- go beyond what is required under the law when responding to demands from any agency or authority for access to customer data; or
- accept any instruction from any agency or authority acting beyond its jurisdiction or legal mandate.

We do:

- insist that all agencies and authorities comply with legal due process;
- scrutinise and, where appropriate, challenge the legal powers used by agencies and authorities in order to minimise the impact of those powers on our customers' right to privacy and freedom of expression;
- honour international human rights standards to the fullest extent possible whenever domestic laws conflict with those standards;
- communicate publicly any threats or risks to our employees arising as a consequence of our commitment to these principles, except where doing so would increase those risks; and
- seek to explain publicly the scope and intent of the legal powers available to agencies and authorities in all countries where it is lawful to do so.

Our policy provides everyone who works for Vodafone with a global governance framework and a set of criteria which must be applied to all interactions with agencies and authorities. In defining our policy (which we update regularly as laws and technologies evolve), we have three objectives, to:

Ensure a robust assessment of the scope of the law
We seek to have as clear an understanding as possible of the scope of – and limits on – the legal powers granted to each country's agencies and authorities in order to ensure we do not exceed what is lawfully required when responding to a demand for assistance.

Ensure appropriate internal oversight and accountability
Vodafone's overall approach to engagement with agencies and authorities is overseen at the most senior level of executive management to ensure effective governance and accountability. However, it is important to note that individual directors' knowledge of specific demands, systems and processes will be limited as a consequence of the restrictions on internal disclosure outlined above.

Address the complexities of law enforcement across multiple countries
Laws designed to protect national security and prevent or investigate crime vary greatly between countries, even within the EU. As a global business operating under local laws in multiple countries and cultures, Vodafone faces a constant tension in seeking to enforce a set of global principles and policies which may be at odds with the attitudes, expectations and working practices of governments, agencies and authorities in some countries. Our global governance framework is designed to manage that tension in a manner which protects our customers and reduces the risks to our employees without compromising our principles.

Privacy and security – Law Enforcement Disclosure report

Communications technology and governments

It is inevitable that legislation lags behind technological innovation in the fast-moving and complex era of internet protocol-based networks, cloud technologies and the proliferation of connected devices in an 'internet of things'. We recognise that agencies and authorities can face significant challenges in trying to protect the public from criminals and terrorists within a legislative framework that pre-dates many of the technologies that are now central to people's daily lives.

We think many governments could do more to ensure that the legal powers relied upon by agencies and authorities are fit for the internet age. In our view, legislative frameworks must be:

- tightly targeted to achieve specific public protection aims, with powers limited to those agencies and authorities for whom lawful access to customer data is essential rather than desirable;
- proportionate in scope and defined by what is necessary to protect the public, not by what is technically possible; and
- operationally robust and effective, reflecting the fact that households access the internet via multiple devices – from games consoles and TVs to laptops, tablets and smartphones – and each individual can have multiple online accounts and identities.

We also believe that governments should:

- balance national security and law enforcement objectives against the state's obligation to protect the human rights of all individuals;
- require all relevant agencies and authorities to submit to regular scrutiny by an independent authority empowered to make public – and remedy – any concerns identified;
- enhance accountability by informing those served with demands of the identity of the relevant official who authorised a demand and by providing a rapid and effective legal mechanism for operators and other companies to challenge an unlawful or disproportionate demand;
- amend legislation which enables agencies and authorities to access an operator's communications infrastructure without the knowledge and direct control of the operator, and take steps to discourage agencies and authorities from seeking direct access to an operator's communications infrastructure without a lawful mandate;
- seek to increase their citizens' understanding of the public protection activities undertaken on their behalf by communicating the scope and intent of the legal powers enabling agencies and authorities to access customer data; and
- publish regular updates of the aggregate number of law enforcement demands issued each year – meeting the proposed criteria we specify earlier in this report – or at the least allow operators to publish this information without risk of sanction and – as we also explain earlier – on the basis of an agreed cross-industry methodology.

Separately, it is important to note that there can be considerable capital costs associated with technical compliance with law enforcement demands, which an operator is usually unable to recover. There are also considerable operating costs, which an operator may be able to recover from the government in a minority of cases, but most of which cannot be recovered. Vodafone therefore does not – and cannot – seek to make a profit from law enforcement assistance.

Agency and authority powers: The legal context

Vodafone is headquartered in the UK: however, in legal terms, our business consists largely of separate subsidiary companies, each of which operates under the terms of a licence or authorisation issued by the government of the country in which that subsidiary is located. Whilst there are some laws which apply across some or all of our businesses (for example, our European operating companies are subject to EU law as well as local laws, and laws such as the UK Bribery Act apply to all our operations), it is important to note that each subsidiary is established in, and operated from, the local market it serves and is subject to the same domestic laws as any other local operator in that country.

All countries have a wide range of domestic laws which govern how electronic communications networks must operate and which determine the extent to which law enforcement agencies and government authorities can intrude into or curtail privacy or freedom of expression.

In some countries those powers are contained within specialist statutes. In others, they may be set out in the terms of a communications company's operating licence. They may also be distributed across a wide range of legislative orders, directives and other measures governing how agencies and authorities carry out their functions.

However enacted, these powers are often complex, opaque and convoluted. A comprehensive catalogue of all applicable laws across all of our countries of operation would be so vast as to be inaccessible to all but the most determined of legal academics: for that reason, in our country-by-country law enforcement disclosure section we have focused on the most salient legislation only. Even with a focus on the most relevant legislative elements alone, the laws can be difficult for anyone other than a specialist lawyer to understand – and sometimes even the specialists can struggle. A summary of the relevant legislation, country by country, can be found in the Annexe.

Despite this complexity, there are a number of areas which are common to many of the legislative frameworks in our countries of operation, the most significant of which we summarise below.

Provision of lawful interception assistance

In most countries, governments have powers to order communications operators to allow the interception of customers' communications. This is known as 'lawful interception' and was previously known as 'wiretapping' from a past era when agents would connect their recording equipment to a suspect's telephone line. Lawful interception requires operators to implement capabilities in their networks to ensure they can deliver, in real time, the actual content of the communications (for example, what is being said in a phone call, or the text and attachments within an email) plus any associated data to the monitoring centre operated by an agency or authority.

Lawful interception is one of the most intrusive forms of law enforcement assistance, and in a number of countries agencies and authorities must obtain a specific lawful interception warrant in order to demand assistance from an operator. In some countries and under specific circumstances, agencies and authorities may also invoke broader powers when seeking to intercept communications received from or sent to a destination outside the country in question. A number of governments have legal powers to order an operator to enable lawful interception of communications that leave or enter a country without targeting a specific individual or set of premises.

Technical implementation of lawful interception capabilities

In many countries, it is a condition of an operator's licence that they implement a number of technical and operational measures to enable lawful interception access to their network and services quickly and effectively on receipt of a lawful demand from an agency or authority with the appropriate legal mandate.

Wherever legally permitted to do so, we follow the lawful interception technical standards set down by the European Telecommunications Standards Institute (ETSI), which define the separation required between the agency or authority monitoring centre and the operator's network. The ETSI standards are globally applicable across fixed line, mobile, broadcast and internet technologies, and include a formal handover interface to ensure that agencies and authorities do not have direct or uncontrolled access to the operators' networks as a whole. We continuously encourage agencies and authorities in our countries of operation to allow operators to conform to ETSI technical standards when mandating the implementation of lawful interception functionality within operators' networks.

In most countries, Vodafone maintains full operational control over the technical infrastructure used to enable lawful interception upon receipt of an agency or authority demand. However, in a small number of countries the law dictates that specific agencies and authorities must have direct access to an operator's network, bypassing any form of operational control over lawful interception on the part of the operator. In those countries, Vodafone will not receive any form of demand for lawful interception access as the relevant agencies and authorities already have permanent access to customer communications via their own direct link. We describe above our views on those arrangements and explain the restrictions imposed on internal discussion of the technical and operational requirements on the Vodafone website.

Vodafone's networks are designed and configured to ensure that agencies and authorities can only access customer communications within the boundaries of the country in question. They cannot access customer communications on other Vodafone networks in other countries.

Privacy and security – Law Enforcement Disclosure report

Disclosure of communications-related data ('metadata')

Whenever a device accesses a communications network, small packets of data related to that device's activities are logged on the systems of the operator responsible for the network. This 'metadata' is necessary for the network to function effectively; for example, in order to route a call to a mobile phone, the network needs to know the mobile network cell site that the device is connected to. Operators also need to store metadata – such as information about call duration, location and destination – to ensure customers are billed correctly. This metadata can be thought of as the address on the outside of an envelope; the communications content (which can be accessed via a lawful interception demand, as explained above) can be thought of as the letter inside the envelope.

It is possible to learn a great deal about an individual's movements, interests and relationships from an analysis of metadata and other data associated with their use of a communications network, which we refer to in this report generally as 'communications data' – and without ever accessing the actual content of any communications. In many countries, agencies and authorities therefore have legal powers to order operators to disclose large volumes of this kind of communications data.

Lawful demands for access to communications data can take many forms. For example, police investigating a murder could require the disclosure of all subscriber details for mobile phone numbers logged as having connected to a particular mobile network cell site over a particular time period, or an intelligence agency could demand details of all users visiting a particular website. Similarly, police dealing with a life-at-risk scenario, such as rescue missions or attempts to prevent suicide, require the ability to demand access to this real-time location information.

In a small number of countries, agencies and authorities have direct access to communications data stored within an operator's network. In those countries, Vodafone will not receive any form of demand for communications data access as the relevant agencies and authorities already have permanent access to customer communications via their own direct link.

Retention of communications data

Communications operators need to retain certain communications data for operational reasons, as described above. Subject to any applicable privacy or data protection laws, operators may also use communications data for marketing and other business purposes, for example, to promote certain products or services likely to appeal to a particular customer based on their previous activity. Vodafone has developed strict rules governing the use of communications data for marketing purposes which we explain in detail in the Privacy and security of our sustainability report.

In some countries, operators are required by law to retain communications data for a specific period of time solely in order to fulfil the lawful demands of agencies and authorities who require access to this data for investigation purposes. For example, since 2006, EU legislation (the Data Retention Directive 2006/24/EC) has required Member States to implement laws that mandate the retention of certain communications data. However, a recent European Court of Justice ruling has found that the Data Retention Directive is incompatible with the Charter of Fundamental Rights of the European Union. The full implications of this ruling for Member States with data retention laws derived from the Directive are still being considered by governments at the time of the publication of this report.

In addition, in many countries mobile operators are obliged to collect information to verify customers' identities. This is primarily to counter the use of anonymous pre-paid mobile phone services where no identity information is otherwise needed to bill for the service.

Decryption of protected data

Electronic communications may be encrypted in some form. This can prevent agencies and authorities from reading the data disclosed to them under applicable legal powers. Encryption can be applied by the operator of the communications network, or it can be applied by the many devices, services and applications used by customers to encrypt data that is transmitted and stored. Several countries empower agencies and authorities to require the disclosure of the encryption 'keys' needed to decrypt data. Non-compliance is a criminal offence. It is important to note that an operator typically does not hold the key for data that has been encrypted by devices, services and applications which the operator does not control: furthermore there is no legal basis under which the operator could seek to gain access to those keys.

Search and seizure powers

In most countries, the courts have the power to issue a variety of search and seizure orders in the context of legal proceedings or investigations. Those orders can extend to various forms of customer data, including a company's business records. The relevant legal powers may be available to members of the public in the course of civil or criminal legal proceedings as well as to a wide range of agencies and authorities.

Privacy and security – Law Enforcement Disclosure report

National security orders

The protection of national security is a priority for all governments. This is reflected in legislative frameworks which grant additional powers to agencies and authorities engaged in national security matters which typically exceed those powers available for domestic law enforcement activities.

For example, in many countries, domestic law enforcement legislation seeks to achieve some form of balance between the individual's right to privacy and society's need to prevent and investigate crime. Those considerations have much less weight in the context of threats to the state as a whole, particularly when those threats are linked to foreign nationals in foreign jurisdictions.

Powers to block or restrict access to communications

IP/URL content blocking and filtering

Some forms of internet content may infringe a country's laws or social norms. Consequently, many countries have laws which enable agencies and authorities to mandate a block on access to content on certain sites (identified by their IP address ranges or URLs), typically by ordering communications providers to apply a filter on their networks. Child abuse content is widely blocked – including on a voluntary basis under the system administered by the Internet Watch Foundation – but other content may be filtered according to a 'block list' maintained by the relevant agencies or authorities.

Take-down of particular services

Many countries empower agencies and authorities to order the take-down of specific electronic communications services for reasons such as a government's desire to restrict access to information it considers harmful to social order. Messaging services and social networks are familiar targets for these take-down actions, although short of a complete network shutdown (addressed below) these measures rarely prove effective over the long-term given the ease with which internet traffic can be re-routed dynamically.

A number of countries also retain legal powers requiring mobile operators to prioritise communications from designated SIMs in mobile phones used by the emergency services at the scene of a major incident where networks can become congested. Whilst such powers are relatively commonplace, in reality they are rarely used and are only effective if the emergency services have supplied operators with an up-to-date list of the SIMs to be prioritised.

Emergency or crisis powers

Many countries have special legal powers that can be invoked at a time of national crisis or emergency, such as a major natural disaster or outbreak of violent civil unrest. The use of those powers typically requires formal approval from the country's parliament (or legislative equivalent). Once invoked, agencies and authorities are empowered to take direct control of a wide range of activities in order to respond to the crisis or emergency.

Whilst emergency or crisis powers are intended to be used for a limited period of time, their effects can be significant. These laws can be used to restrict or block all forms of electronic communication, either in a specific location or across the country as a whole. In January 2011, the Egyptian government ordered all operators – including Vodafone – to shut down their networks entirely. An overview of these events and Vodafone's response can be found on the Vodafone website.

Further details about the legal powers available to agencies and authorities in each of our countries of operation are set out in our country-by-country law enforcement disclosure section, together with statistical information about the number of demands received.

Notes:

1. Source: ITU: www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Country-by-country disclosure of law enforcement assistance demands

Introduction

As explained earlier in this report, Vodafone's global business consists largely of a group of separate subsidiary companies, each of which operates under the terms of a licence or other authorisation issued by the government of the country in which the subsidiary is located, and each of which is subject to the domestic laws of that country.

In this section of the report, we provide a country-by-country insight into the nature of the local legal regime governing law enforcement assistance, together with an indication of the volume of each country's agency and authority demands wherever that information is available and publication is not prohibited. In addition, a summary of some of the most relevant legal powers in each of our countries of operation can be found in our legal Annexe.

As we explain earlier in this report, this has been a difficult section to compile. There is no established model to follow: few international communications operators have published a country-by-country report of this kind; and very few have done so on the basis of data gathered by the local licensed communications operator. Additionally, there are no standardised methods for categorising the type and volume of agency and authority demands; different governments, parliaments, regulators, agencies and authorities apply a variety of definitions when authorising or recording the types of demands outlined earlier in this report, as do operators themselves when receiving and recording those demands.

The need for governments to balance their duty to protect the state and its citizens against their duty to protect individual privacy is now the focus of a significant global public debate. We hope that – despite the shortcomings described above – the country-by-country disclosures in this report will help inform that debate.

How we prepared this report

Each of our local operating businesses has a nominated Disclosure Officer responsible for the management and administration of law enforcement assistance in response to a demand. The information collated and published here (wherever available and wherever publication has not been prohibited) has been overseen by the relevant Disclosure Officer. As explained earlier in this report, only local Vodafone employees with a high level of government security clearance will ever be made aware of specific lawful demands issued by agencies and authorities, and even then they will not typically be made aware of the context of any demand. It is therefore not possible for the external assurers for the Vodafone Group Sustainability Report, EY, to provide any form of independent verification of the statistical information published in this section. However, the integrity and operation of our law enforcement disclosure systems are subject to verification under Vodafone's own internal audit controls.

For the two categories of agency and authority demand reported here – lawful interception and communications data (as explained earlier in this report) – we have robust processes in place to manage and track each demand and to gather statistical information on aggregate volumes.

It should be noted that, whilst the statistics for communications data demands are overwhelmingly related to communications metadata, the statistics we report also include demands for other types of customer data such as name, physical address and services subscribed. Our reporting systems do not necessarily distinguish between the types of data contained in a demand, and in some countries a single demand can cover several different types of data.

We have also conducted a global internal review to analyse, on a country-by-country basis, the extent to which we can lawfully publish aggregate volumes of law enforcement assistance demands at a local level. That review involved Vodafone's senior local legal counsel in each of the 29 countries covered here.

Additionally, we instructed the international law firm, Hogan Lovells[2], to support us in reviewing and verifying the legal opinions received from each of our operating country businesses. Hogan Lovells coordinated this work through its network of local law firms across Vodafone's countries of operation, with each firm selected for its expertise in the areas of law relevant to this report. Hogan Lovells subsequently supported Vodafone in creating a legal report for each country (extracts of which are published below, where relevant), and the legal Annexe also sets out a more detailed overview of some of the most important legal powers in each country.

In many countries, there is a lack of legal clarity regarding disclosure of the aggregate number of law enforcement demands. We have therefore contacted governments to ask for guidance. Some have responded, and their views are summarised in this report. Others have simply declined to reply to our enquiries altogether or have been reluctant to provide an indication of their perspectives. In a small number of countries where the government does publish statistics but where there are concerns regarding the methodology used in recording and/or reporting this information, we summarise in this report the measures underway to enhance transparency in future. Further information about our approach under those circumstances are set out earlier in this report. Finally, in countries experiencing periods of significant political tension, it has proven to be challenging to ask any questions related to national security and criminal investigation matters without potentially putting Vodafone employees at risk of harassment or some form of sanction.

Privacy and security – Law Enforcement Disclosure report

Explanation of the information presented

In each country and for each of the two categories of law enforcement demands issued, there are a number of different outcomes arising from our enquiries.

Wherever there are no restrictions preventing publication and there are no alternative sources of information indicating total demand volumes across all operators in the country as a whole, we have published the data available from our own local operating business indicating the cumulative number of demands received by Vodafone during the period under review. However, note our concerns about the shortcomings inherent to this approach, as explained earlier in this report.

There are six circumstances under which we have not published Vodafone's own statistical information for a specific country, as set out below.

1. **Vodafone disclosure unlawful**
   The law prohibits disclosure of the aggregate demand information held by Vodafone as well as any disclosure related to the mechanisms used to enable agency and authority access, as explained earlier in this report. This is particularly the case in matters related to national security. Wherever this is the case, we cite the relevant law that restricts us from disclosure, either in the main text or in the Annexe.
2. **No technical implementation of lawful interception**
   In some countries, there is no legal provision for implementation or we have not been required to implement the technical requirements necessary to enable lawful interception and therefore have not received any agency or authority demands for lawful interception assistance. This includes circumstances under which lawful interception powers exist under the law but the technical arrangements to conduct this have not been mandated.
3. **Awaiting guidance**
   The law on disclosure is unclear, and we are still awaiting guidance from the government or a relevant agency or authority as to whether or not we can disclose this information.
4. **Unable to obtain guidance**
   The law on disclosure is unclear and we have been unable to engage with the government or a relevant agency or authority to discuss options for publication during a period of political tension and consequent risk to our employees.
5. **Cannot publish**
   Although local laws do not expressly prohibit disclosure, the authorities have told us directly that we cannot disclose this information.
6. **Government publishes**
   In a number of countries, the government, parliament or a credible independent body such as a regulator already publishes statistical information for certain types of demand issued to all operators in that country. Wherever this is the case, we provide a link to the information available online. In some countries – and where relevant – we also provide additional commentary on the status of that third-party information. Our views on disclosure of relevant information by governments rather than by operators are summarised earlier in this report.

Notes:

2. Vodafone are grateful to Hogan Lovells for its assistance in collating the legal advice underpinning this report including the country-by-country legal annexe. However, in doing so, Hogan Lovells has acted solely as legal adviser to Vodafone. This report 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.

Privacy and security – Law Enforcement Disclosure report – Country-by-country section

Country-by-country disclosure

The following tables offer a country-by-country insight into the nature of the local legal regime governing law enforcement assistance, together with an indication of the volume of each country's agency and authority demands, wherever that information is available and publication is not prohibited. The links to the individual government reports that are referenced in many of the country tables can be found in the online report at www.vodafone.com/sustainability/lawenforcement

A summary of the relevant legislation, on a country-by-country basis, can be found in the legal annexe, which can also be found in the online version of this report.

Albania		
Type of demand		
	Lawful Interception	Communications Data
Statistics	Vodafone disclosure unlawful (1)	5,778 (2)
Key Note (1)	It is unlawful to disclose any aspect of how lawful interception is conducted.	
Key Note (2)	The legal position is unclear regarding whether or not it would be lawful for Vodafone to disclose statistics related to agency and authority communications data demands. We asked the authorities for guidance and have been informed that we can disclose this information.	

Australia		
Type of demand		
	Lawful Interception	Communications Data
Statistics	Government publishes (1) Further action to follow (2)	Government publishes (1) Further action to follow (2)
Key Note (1)	The Australian Communications and Media Authority and the Australian Attorney General's Department publish statistical information related to lawful interception and communications data demands issued by agencies and authorities.	
Key Note (2)	During the course of preparing this report, another local operator published information relating to some of the statistical data it holds for its own operations. We have approached the Attorney General's Department to work with industry and government on a common methodology to be followed in the recording and disclosure of this information. We will update this section of the report in future once we have further information as a consequence of that process.	

Belgium		
Type of demand		
	Lawful Interception	Communications Data
Statistics	No technical implementation (1)	2
Key Note (1)	We have not implemented the technical requirements necessary to enable lawful interception and therefore have not received any agency or authority demands for lawful interception assistance.	

Czech Republic		
Type of demand		
	Lawful Interception	Communications Data
Statistics	7,677	Government publishes (1)
Key Note (1)	The Czech Telecommunications Office publishes statistical information related to communications data demands issued by agencies and authorities.	

Democratic Republic of the Congo		
Type of demand		
	Lawful Interception	Communications Data
Statistics	No technical implementation (1)	436
Key Note (1)	We have not implemented the technical requirements necessary to enable lawful interception and therefore have not received any agency or authority demands for lawful interception assistance.	

Privacy and security – Law Enforcement Disclosure report – Country-by-country section

Egypt		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	Vodafone disclosure unlawful (1)	Vodafone disclosure unlawful (1)
Key Note (1)	Whilst the precise legal position regarding disclosure of aggregate statistical information is unclear, local criminal laws contain a large number of provisions prohibiting the disclosure of national security-related material and other matters related to law enforcement. The disclosure of statistical information related to agency and authority demands is therefore very likely to be considered to be a violation of such provisions.	

Fiji		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	No technical implementation (1)	760
Key Note (1)	We have not implemented the technical requirements necessary to enable lawful interception and therefore have not received any agency or authority demands for lawful interception assistance.	

France		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	No technical implementation (1)	3
Key Note (1)	We have not implemented the technical requirements necessary to enable lawful interception and therefore have not received any agency or authority demands for lawful interception assistance.	

Germany		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	Government publishes (1) Further action to follow (2)	Government publishes (1) Further action to follow (2)
Key Note (1)	The German Federal Office of Justice publishes annual statistics related to agency and authority lawful interception demands. The German Federal Office of Justice publishes annual statistics related to agency and authority demands for access to communications data. In its annual report, the Federal Network Agency (Bundesnetzagentur) publishes statistics related to access by the Regulatory Authority to communications data stored in accordance with Article 112 of the German Telecommunications Act (TKG).	
Key Note (2)	The legal position is unclear regarding whether or not it would be lawful for Vodafone to disclose statistics related to agency and authority lawful interception and communications data demands. Section 113(4) of the German Telecommunications Act (TKG) outlines that communication service providers must not disclose the fact that there was a request for information or that they provided such information to the concerned person or third parties. Section 15(2) of the Telecommunications Interception Ordinance (TKÜV) prohibits the operator of a telecommunication system from disclosing information related to lawful interception, the number of present or past lawful interceptions, as well as the time periods in which lawful interception measures were conducted. Although there is no legal precedent, the confidentiality obligation in Section 113(4) TKG could be interpreted by German courts or authorities to extend to a prohibition of the disclosure of aggregate demand statistics. If it is unlawful to disclose the existence of a single or particular demand for communications data, to disclose aggregate statistics would indicate that there have clearly been a number of such demands. Given the lack of clarity in the law, we asked the authorities for guidance and were advised that we were not permitted to disclose any of the information we hold related to agency and authority demands for lawful interception and access to communications data. Subsequent to this, other operators in Germany began to publish information related to some of the law enforcement demands they have received and we understand that publication may now be permissible. However, we are concerned that the information disclosed to date may in fact act as a significant barrier to the kind of meaningful transparency necessary to maintain public trust in Germany. Whilst other operators appear to be following a methodology similar to that used by Vodafone Germany in recording statistics related to law enforcement demands (and indeed the demand volumes recorded for Vodafone Germany are closely comparable to those reported by other operators of a similar scale), other operators' disclosures to date: • present only a partial view of law enforcement demands (for example, they exclude the effect of German agency and authority automated access systems which allow rapid and large-scale interrogation of a central database of customer records); • cannot be reconciled with the authorities' publication of the number of warrants issued each year (with the potential for significant confusion as a result of wide variations in recording and reporting approaches, as explained earlier in this report); and • remain potentially unlawful and therefore subject to prohibition in future, notwithstanding the authorities' assurances received immediately prior to publication of this report. We will therefore engage with other German operators and the German authorities to seek consensus on a more robust and consistent local disclosure framework in future. We will update this section of the report once we have further information as a consequence of that process.	

Privacy and security – Law Enforcement Disclosure report – Country-by-country section

Ghana		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	No technical implementation (1)	Awaiting guidance (2)
Key Note (1)	We have not implemented the technical requirements necessary to enable lawful interception and therefore have not received any agency or authority demands for lawful interception assistance.	
Key Note (2)	The legal position is unclear regarding whether or not it would be lawful for Vodafone to disclose statistics related to agency and authority communications data demands. Under the Electronic Communications Act, 2008 ("ECA"), certain classes of information which are deemed to be of importance to the protection of national security may be declared to be critical electronic records and subject to restrictions in respect of access, transfer and disclosure. Under section 56 of the ECA, the Minister for Communications may by notice in the Gazette (the official government publication) declare certain classes of information which are deemed to be of importance to the protection of national security to be critical electronic records. Section 59 of the ECA therefore provides for the setting of minimum standards in respect of access to, transfer and control of a critical database. Additionally, section 60 of the ECA imposes restrictions on the disclosure of information in a critical database to persons other than the employees of the National Information Technology Agency, a law enforcement agency, a ministry, department or other government agency. As a result, if the aggregate data in respect of the above agency and authority demands are designated as critical electronic records, the government will be able to prevent Vodafone from publishing them. We have asked the authorities for guidance: however, we have not yet received a reply. We will update this section of the report in future if further information becomes available.	

Greece		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	Government publishes (1)	Government publishes (1)
Key Note (1)	The Hellenic Authority for Communication Security and Privacy (ADAE) publishes statistical information related to lawful interception and communications data demands issued by agencies and authorities.	

Hungary		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	Vodafone disclosure unlawful (1)	75,938 (2)
Key Note (1)	It is unlawful to disclose any aspect of how lawful interception is conducted.	
Key Note (2)	Under s.62 of the National Security Service Act, if the intelligence services demand information from communications service providers, the service provider is not allowed to disclose any information (including aggregate data or statistics) in relation to such cooperation without the prior explicit permission of the competent minister or director general of the particular intelligence agency. The statistics disclosed here therefore do not include demands for access to communications data related to matters of national security.	

India		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	Vodafone disclosure unlawful (1)	Vodafone disclosure unlawful (1)
Key Note (1)	Section 5 (2) of the Indian Telegraph Act 1885 – read with rule 419 (A) of Indian Telegraph (Amendment) Rules 2007 obliges telecommunications service providers to "maintain extreme secrecy" in matters concerning lawful interception. Further, under Rule 25(4) of the IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (Interception Rules) and Rule 11 of the IT (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 (the 'Traffic Data Rules'), "strict confidentiality shall be maintained" in respect of directions for lawful interception, monitoring, decryption or collection of data traffic. These prohibitions extend to the very existence of such directions, and could therefore authorise the government to prevent the publication of aggregate data relating to the number of directions received by the licensee. In addition, in respect of lawful interception directions made under the Information Technology Act, 2000 (IT Act) and its associated Rules, the government can prevent the publication of aggregate data in relation to lawful interception and other data disclosure demands from the government and law enforcement agencies. Finally, under Clause 40.5 of the Unified Access Service License (UASL: the licence governing access service in India), and Clause 33.5 of the Internet Service Provider (ISP) License (the licence governing internet access service in India), the licensee is bound to maintain the secrecy and confidentiality of any confidential information disclosed to the licensee for the proper implementation of the licences. Aggregate data regarding agency and authority demands come under the purview of these provisions.	

Privacy and security – Law Enforcement Disclosure report – Country-by-country section

Ireland		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	Cannot disclose (1)	4,124
Key Note (1)	Whilst local laws do not expressly prohibit disclosure, we asked the authorities for guidance and have been informed that we cannot disclose this information.	

Italy		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	Government publishes (1)	605,601
Key Note (1)	The Italian Ministry of Justice publishes statistics on the number of lawful interception demands issued by agencies and authorities.	

Kenya		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	No technical implementation (1)	Unable to obtain guidance (2)
Key Note (1)	Local operators are legally prohibited under s.31 of the Kenya Information & Communication Act from implementing the technical requirements necessary to enable lawful interception. We have therefore not received any agency or authority demands for lawful interception assistance.	
Key Note (2)	The legal position is unclear regarding whether or not it would be lawful for Safaricom (Vodafone's local associate operator) or Vodafone to disclose statistics related to agency and authority communications data demands. Section 3 of the Official Secrets Act provides certain instances where publication or disclosure of information is deemed an offence. The broad language of this Act includes publication of data collected by the security agency in Kenya. In addition, Section 37 of the National Intelligence Service Act (Act No. 28 of 2012) ("NIS Act") limits a person's constitutional right of access to information where such information is classified. When read with the Official Secrets Act (Cap. 187 Laws of Kenya), the government can prevent the publication of such data if such publication will be prejudicial to safety and the interest of the Republic of Kenya. The NIS Act defines "classified information" as information of a particular security classification, whose unauthorised disclosure would prejudice national security. While the NIS Act does not define what would be deemed to prejudice national security, the 2010 Constitution of Kenya provides how national security shall be promoted and guaranteed. A National Security Council exists to exercise supervisory control over national security matters in Kenya and to determine what may prejudice national security. It is therefore under this umbrella (prejudice to national security) that the government can prevent the publication of various agency and authority demands. It may follow that where there is no prejudice to national security that these restrictions do not apply, albeit that what amounts to a prejudice to national security is legally undefined. Under the current circumstances, we have concluded that it will not be possible to engage with government, agencies and authorities on these matters at this point. We will update this section of the report in future if circumstances change.	

Lesotho		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	No technical implementation (1)	488
Key Note (1)	We have not implemented the technical requirements necessary to enable lawful interception and therefore have not received any agency or authority demands for lawful interception assistance.	

Malta		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	Vodafone disclosure unlawful (1)	3,773 (2)
Key Note (1)	It is unlawful to disclose any aspect of how lawful interception is conducted.	
Key Note (2)	The legal position is unclear regarding whether or not it would be lawful for Vodafone to disclose statistics related to agency and authority communications data demands. We asked the authorities for guidance and have been informed that we can disclose this information.	

Privacy and security – Law Enforcement Disclosure report – Country-by-country section

Mozambique		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	No technical implementation (1)	Unable to obtain guidance (2)
Key Note (1)	We have not implemented the technical requirements necessary to enable lawful interception and therefore have not received any agency or authority demands for lawful interception assistance.	
Key Note (2)	The legal position is unclear regarding whether or not it would be lawful for Vodafone to disclose statistics related to agency and authority communications data demands. Under the current circumstances, it has not been possible to engage with the government on these matters. We will update this section of the report in future if further information becomes available.	

Netherlands		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	Vodafone disclosure unlawful (1) Government publishes (2) Further action to follow (3)	Government publishes (2) Further action to follow (3)
Key Note (1)	Article 85 of the Intelligence and Security Services Act 2002 ('Wet op de inlichtingen en veiligheidsdiensten 2002' or 'ISSA'), requires all persons involved in the execution of the ISSA to keep the data obtained confidential. It would be unlawful for Vodafone to disclose statistical information related to lawful interception demands issued by agencies and authorities under the ISSA.	
Key Note (2)	The Dutch Ministry of Justice publishes statistical information related to lawful interception and communications data demands issued by agencies and authorities.	
Key Note (3)	As explained earlier in the report, we believe that the wide variations in methodology used by operators, governments and others in recording and reporting this statistical information amounts to a serious barrier to meaningful public transparency. We wrote to the Ministry of Security and Justice to urge further action by government in this area. In response, the Ministry outlined its aim to improve public transparency and committed to form a cross-functional working group – including Dutch operators – to consider options to increase the quality of public transparency. We will update this section of the report in future once we have further information as a consequence of that process.	

New Zealand		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	Government publishes (1)	Government publishes (1)
Key Note (1)	Statistical information related to lawful interception and communications data demands issued by agencies and authorities is published by the following four organisations: The New Zealand Police The New Zealand Security Intelligence Service The New Zealand Serious Fraud Office The New Zealand Customs Service	

Portugal		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	Government publishes (1)	28,145 (2)
Key Note (1)	The Portuguese Ministry of Internal Affairs publishes statistical information related to lawful interception demands issued by agencies and authorities.	
Key Note (2)	We asked the authorities for guidance and have been informed that we can disclose this information.	

Privacy and security – Law Enforcement Disclosure report – Country-by-country section

Qatar		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	Vodafone disclosure unlawful (1)	Cannot disclose (2)
Key Note (1)	It is unlawful to disclose any aspect of how lawful interception is conducted.	
Key Note (2)	The legal position is unclear regarding whether or not it would be lawful for Vodafone to disclose statistics related to agency and authority communications data demands. Article 59 of the Qatar Telecommunication Law states that telecommunications service providers must comply with the requirements of the security authorities 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 interested in "State security" can rely on Article 59 alongside use any enforcement powers vested directly in that government authority. We asked the authorities for guidance and have been informed that we cannot disclose this information.	

Romania		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	Vodafone disclosure unlawful (1)	Awaiting guidance (2)
Key Note (1)	It is unlawful to disclose any aspect of how lawful interception is conducted.	
Key Note (2)	The legal position is unclear regarding whether or not it would be lawful for Vodafone to disclose statistics related to agency and authority communications data demands. Article 142(3) and Article 152 (3) of the Criminal Procedure Code (Law 135/2010) states that communication service providers are required to cooperate with criminal prosecution authorities with regard to lawful interception and the supply of retained communications data must keep the relevant operation a secret. Publishing aggregate statistics could potentially violate this obligation. We have asked the authorities for guidance however, we have not yet received a reply. We will update this section of the report in future if further information becomes available.	

South Africa		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	Vodafone disclosure unlawful (1)	Vodafone disclosure unlawful (1)
Key Note (1)	Section 42 of the Regulation on Interception of Communication and Provision of Communication-related Information Act 2002 prohibits the disclosure of any information received pursuant to the Act. This includes, by virtue of Section 42(3), the disclosure of the fact that any demand for lawful interception or communications data has been issued under the Act. Accordingly, to publish aggregate statistics would be to disclose the existence of one or more lawful interception or communications data demands.	

Spain		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	24,212 (1)	48,679 (1)
Key Note (1)	The legal position is unclear regarding whether or not it would be lawful for Vodafone to disclose statistics related to agency and authority lawful interception and communications data demands. We asked the authorities for guidance and have been informed that we can disclose this information.	

Tanzania		
	Type of demand	
	Lawful Interception	Communications Data
Statistics	No technical implementation (1)	98,765
Key Note (1)	We have not implemented the technical requirements necessary to enable lawful interception and therefore have not received any agency or authority demands for lawful interception assistance.	

Privacy and security – Law Enforcement Disclosure report – Country-by-country section

Turkey		
	Type of demand	
	Lawful Interception	**Communications Data**
Statistics	Vodafone disclosure unlawful (1)	Vodafone disclosure unlawful (1)
Key Note (1)	It is unlawful to disclose any aspect of how lawful interception or access to communications data are conducted.	

United Kingdom		
	Type of demand	
	Lawful Interception	**Communications Data**
Statistics	Vodafone disclosure unlawful (1) Government publishes (2)	Government publishes (2)
Key Note (1)	Section 19 of the Regulation of Investigatory Powers Act 2000 prohibits disclosing the existence of any lawful interception warrant and the existence of any requirement to provide assistance in relation to a warrant. This duty of secrecy extends to all matters relating to warranted lawful interception. Data relating to lawful interception warrants cannot be published. Accordingly, to publish aggregate statistics would be to disclose the existence of one or more lawful interception warrants.	
Key Note (2)	The Interception of Communications Commissioner's Office publishes statistical information related to lawful interception and communications data demands issued by agencies and authorities.	

For a summary of the most important legal powers relating to law enforcement demands on a country-by-country basis, see our Law Enforcement Disclosure report country-by-country legal annexe which is available on our website at www.vodafone.com/sustainability/lawenforcement

Law Enforcement Disclosure Report

Legal Annexe
June 2014

Vodafone
Power to you

Law Enforcement Disclosure Report Legal Annexe

Contents

Vodafone Law Enforcement Disclosure report Country-by-country legal annexe

TRANSPARENCY AND THE LAW

This annexe to Vodafone's Law Enforcement Disclosure report seeks to highlight some of the most important legal powers available to government agencies and authorities seeking to access customer communications across the 29 countries of operation covered in this report.

Whilst the legal powers summarised here form part of local legislation in each of those 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.

Creation of this annexe

This annexe has been compiled by our legal counsel in each of our 29 countries of operation with support from the international law firm, Hogan Lovells* and their network of local law firms. It contains advice on the meaning of some of the most important laws that empower government agencies and authorities to demand access to customer communications. We have outlined some of the most common types of legal powers used to demand assistance from local licensed operators earlier in our Law Enforcement Disclosure report. However, we have not covered other areas, such as the many and varied 'search and seizure' powers, powers to block or take down content or the restriction of access to services.

Compiling this annexe has proven to be a complex task. Vodafone counsel and the external law firms supporting us in this work have had a number of intense debates about the meaning and interpretation of some of the laws which 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. Precise interpretation is difficult, exacerbated further (as we highlight earlier in this report) by significant uncertainty on the part of some governments themselves, when we have sought guidance.

In this annexe, we focus on the three categories of legal power which 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 report. Legal powers under those three categories are specifically relevant to our local licensed communications operator businesses and can usually be found in telecommunications statutes or in the conditions of the licence issued by governments to operators.

Our contribution to the debate

We would emphasise that individual countries' legislation will not always fall neatly under one of these three categories 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 29 countries, we hope that this section of the report will serve as a useful framework for further analysis in future.

As part of our commitment to ensuring this important debate is fully informed, we are making this annexe available under a Creative Commons license and by doing so hope others will re-use and build upon this material to aid greater transparency in this area.

*Vodafone are grateful to Hogan Lovells for its assistance in collating the legal advice underpinning the law enforcement disclosure report and this the country-by-country legal annexe. However, in doing so, Hogan Lovells has acted solely as legal adviser to Vodafone. This report 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.

Countries A-E

Albania

In this report we provide an overview of some of the legal powers under the law of Albania that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

The Interception Law

Article 22 of the 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 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 Article 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, i.e. 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 which requires 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 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 (i.e. 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, 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, data, 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 e-mail 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, propose to the Council of Ministers the measures to be included in the notices issued to the operators.

Additionally, under Law No. 8756, dated 26.3.2001 "On civil emergencies", government authorities have the right to use any private or public means or to cooperate 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.

Australia

In this report we provide an overview of some of the legal powers under the Commonwealth Law of Australia that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

Australia is a Federation containing three separate types of legislation: Commonwealth, State and Territory. This report focuses on the legal powers available under Commonwealth Law.

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 the authorities such help as is reasonably necessary for the purposes of: (i) enforcing the criminal law and laws imposing pecuniary penalties; (ii) protecting the public revenue; and (iii) safeguarding national security. Section 313(7) of the TA specifies that a reference to 'giving help' under section 313(3) of the TIA includes the provision of interception services, including services in executing an interception warrant, and the providing of relevant information about any communication that is lawfully accessed 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) 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 ("**TIA**") gives law enforcement agencies and national security agencies the power to intercept live communications in specified circumstances.

Under Chapter 2, Part 2-2 of the TIA, 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 to ASIO by the Federal Attorney General under sections 9 and 9A of the TIA for national security purposes, and by the Director-General of Security in emergencies under section 10 of the TIA. Under sections 11A, 11B and 11C of the TIA, 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, an officer of ASIO appointed by the Director-General of Security and approved officers and employees of ASIO. A foreign communications warrant issued under section 11C 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 11C(1B) of the TIA). Under section 11B(4)(a) a foreign 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 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 (Part 2-3 of Chapter 2 of the TIA).

Interception of live communications may also be authorised (without a warrant) under section 31A of the TIA by the Attorney-General to enable security authorities for the purpose of developing and testing interception capabilities (Part 2-4 of Chapter 2 of the TIA).

Under Chapter 2, Part 2-5 of the TIA interception warrants may be issued to law enforcement agencies specified by the Minister under section 34, such as 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). Interception warrants may only be issued in relation to the investigation of serious offences as defined in section 5D of the TIA.

Chapter 5 of the TIA imposes obligations on carriers to ensure that it is possible to execute a warrant issued for interception purposes, unless an exception has been granted by the Minister, the Australian Communications and Media Authority ("**ACMA**") or the Attorney-General's Department. 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, 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 Capabilities Plans' ("**IC plan**") with the Communications Access Co-ordinator of the Attorney-General's Department. Part 5-4 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, the Communications Access Co-ordinator may make determinations in relation to delivery capabilities applicable to specified kinds of communication 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 Act 1979

The Australian Security Intelligence Act 1979 ("**ASIO Act**") enables ASIO to use listening devices under warrants issued by the Minister.

Division 2 of Part 3 of the ASIO Act enables an officer, employee or agent of ASIO to use a listening device where issued with a warrant. A warrant may be issued by the Minister upon application by the Director-General where a person is engaged in, or is reasonably suspected by the Director-General of being engaged in activities prejudicial to security. A warrant issued under this section must not exceed a period of 6 months and may be revoked by the Minister at any time before the expiration of the period specified in the warrant. Where a listening device is installed in accordance with the warrant, ASIO may enter any premises for the purpose of recovering a listening device and may use any force that is necessary and reasonable to recover the listening device.

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.

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 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

Telecommunications Act 1997

Carriers have legislative obligations under the TA to provide assistance to law enforcement and national security agencies which includes 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 Telecommunications Universal Services Agency 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)).

Telecommunications (Interception and Access) Act 1979

Chapter 4 of the TIA specifies the circumstances in which information may be voluntarily disclosed to government and law enforcement agencies and the conditions by which authorisations can be issued requiring the disclosure of information.

Sections 174 and 175 of the TIA 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 Secretary, the Deputy Director of Secretary or a specified officer or employee of ASIO. Authorisations may be in respect of existing information or prospective information (specified information or documents that come into existence during the period for which the authorisation is in force).

Sections 177 to 180 of the TIA 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 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.

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

Under Parts 3-2 and 3-3 of Chapter 3 of the TIA, stored communication warrants for law enforcement purposes may be issued to enforcement agencies for the purpose of investigating serious offences and serious contraventions. Enforcement agencies mean criminal law enforcement agencies, civil penalty enforcement agencies (agencies responsible for administrating a law imposing a pecuniary penalty) and public revenue agencies (agencies responsible for administration of a law relating to the protection of the public revenue) (section 282 of the TA). Such agencies include but are not limited to agencies such as the ACCC, Australian Customs Services, the Australian Tax Office, the Australian Securities and Investments Commission (**ASIC**) and similar State and Territory agencies. ASIO can access stored communications using its existing interception warrants (section 109 of the TIA).

Stored communication warrants can be issued by 'eligible 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 3 years. Stored communication warrants may also be issued as part of a statutory civil proceedings which would render the person of interest to a pecuniary penalty.

The Crimes Act

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

The Australian Security Intelligence 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.

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.

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 as well as a number of reporting requirements. These requirements are designed to ensure that appropriate levels of accountability exist.

Under the TIA, 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 reports (such as those maintained by the AFP) and report to the Attorney-General who must table in Parliament each year a report containing specified information (Part 2-7 of Chapter 2 of the TIA).

Part 2-10 of Chapter 2 of the TIA 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 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 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 requires an enforcement agency to give the Minister a written report, no later than 3 months after 30 June, of all authorisations issued under Chapter 4 of the TIA in the preceding financial year. The Minister must then cause a copy of that report to be tabled before Parliament.

Part 3-7 of Chapter 3 of the TIA 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.

The same reporting requirements are placed on 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).

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), 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) or 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/s 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 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.

Belgium

In this report we provide an overview of some of the legal powers under the law of the Belgium that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

Code of Criminal Procedure

The Code of Criminal Procedure provides for the possibility 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 s/he imposes special investigation measures, including interception measures. This order needs to explain why such measure 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, §1 of the Code of Criminal Procedure states that the warrant issued by the examining magistrate and authorising the interception measure 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, §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 requests so.

The Royal Decree of the 9th January 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 down 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 lays down that every electronic communications operator needs to designate one or more persons being charged with the cooperation duty (i.e. 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 lays down 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 of 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 regards 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 examines in its advice 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.

The authorisation needs to be written and contain: (i) a description of the exceptional threats justifying the interception, (ii) reasons why the interception is necessary, (iii) persons or entities whose communications are being

intercepted, (iv) the technical means used to intercept, (v) the period of interception; and (vi) names of the intelligence officers involved in the operation.

With regards to an interception measure (in addition to the article 18/10-authorisation), article 18/17, §1 of the Intelligence and Safety Services Act of 30 November 1998 lays down that the intelligence services can intercept a person's communications. §3 lays down 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 15 October 2010 on specific rules for the legal 'cooperation duty' in case of actions of the intelligence services regarding electronic communications lays down the details of this cooperation duty. Every electronic communications operator needs to designate one or more persons being charged with the cooperation duty (i.e. 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 for interception of private communications or telecommunications following receipt of the written and reasoned decision of the Director-General of the intelligence service.

The Electronic Communications Act 2005

Article125, §2 of the, the Electronic Communications Act of 13 June 2005 (relating to interception demands coming from authorities competent for prosecution and investigation of criminal offences and/or the intelligence service), states that the King determines the modalities for the means to be put in place with a view of identifying, tracking down, localising, getting aware of and intercepting electronic communications. These modalities have been determined in the Royal Decree of 15 October 2010 mentioned above.

Article 127, §1, 2° of the Electronic Communications Act lays down the technical and administrative measures electronic communications operators need to take with a view of being able to identify, track down, intercept and become aware of private communications (upon demand of the competent authorities and/or the intelligence service). If the operator does not take such measures (i.e. internal procedures for dealing with these requests), it is not allowed to offer the electronic communication service in respect of which these measure(s) have not been taken.

2. DISCLOSURE OF COMMUNICATIONS DATA

The Electronic Communications Act of 13 June 2005

This Act contains provisions on the duty of electronic communications operators to provide metadata upon demand of the competent prosecution/investigation authorities (see below – Criminal Procedure Code) and of the intelligence services (see below – Intelligence and Safety Services Act of 30 November 1998).

Article 122, §2 of the Electronic Communications Act of 13 June 2005 lays down that electronic communications operators may be required not to remove or to anonymise their traffic data relating to subscribers or end users, if authorities prosecuting criminal offences or the intelligence services require them to do so.

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

Article 127, §2, 1° lays down the technical and administrative measures electronic communications operators need to take with a view to being able to identify, track down and intercept, private communications. If they do not take such measures (i.e. internal procedures for dealing with these requests), they are not allowed to offer the electronic communication services for which these measure(s) have not been taken. The modalities for 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, §1, 1° of the Royal Decree on legal cooperation duty following legal actions, as well as art. 8, §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.

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 Criminal Procedure Code:

– Art. 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.

– Art. 88 bis: Following a reasoned court order from the examining magistrate, he or she may require an electronic communications operator to provide data allowing identification and location of a subscriber or an electronic communications service.

  For every means of telecommunication used and that is 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 of 30 November 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 lays down that the disclosure of identification and localisation data can only be executed after a written and reasoned decision of 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.

Articles 18/7, §1 of the Intelligence and Safety Services Act of 30 November 1998 lays down that the electronic communications operators have to provide data allowing the identification of a subscriber or user of an electronic communications service as well as the communication of their invoices (the Director-General needs to address a written decision to the operators with a view of obtaining their cooperation, on top of the art. 18/3-decision).

Article 18/8, §1 of the Intelligence and Safety Services Act of 30 November 1998 lays down 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 down the details of these requirements, i.e. this communication of data needs to be done by the Coordination Cell of Justice.

3. NATIONAL SECURITY 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 interest of public security (after consultation within the Council of Ministers).

Civil Contingences 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 customer's communications data in Belgium.

For instance, Article 181 of the Civil Contingencies Act lays down that the Ministers competent for internal affairs 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 regards to the interception measures ordered by the examining magistrate pursuant to the Criminal Code Procedure, the person whose communications have been intercepted can argue that the interception was illegal. He can do this before a pre-trial chamber ("Chambre du conseil/ Raadkamer"), during the pre-sentence stage (before the case is treated on the merits). He can also do this during the treatment of the case on the merits before the Criminal Court, before the Court of Appeal or eventually before the Court of Cassation.

With regards to the interception executed by the intelligence and safety services act of 30 November 1998, there is administrative oversight. Article 18/10, § 6 of the Intelligence and Safety Services Act of 30 November 1998 outlines that, at any time, the members of the Commission can exercise control on the legality of the measures (including the principles of proportionality and subsidiarity). 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) present at the origin of the interception measure no longer exist(s) or that the measure is no longer useful, it ends the interception 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 of another Commission, i.e. 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 the a posteriori control on the interception measures (i.e. the legality and the 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 disclosure was illegal. He can do this before the pre-trial chamber ("Chambre du conseil/Raadkamer"), during the pre-sentence stage (before the case is treated on the merits). He can also do this during the treatment of the case on the merits, before the Criminal Court, before the Court of Appeal or, eventually, before the Court of Cassation.

With regards 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, § 2 at the end of every month, a list of executed measures (among which the disclosure measures) is sent to the Commission. At any time the members of the Commission can exercise control on 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 taking advice from the Commission on the Protection of Privacy ("Privacy Commission")). The Commission prohibits the use of the 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 Contingences Act 2007.

Czech Republic

In this report we provide an overview of some of the legal powers under the law of the Czech Republic that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

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 (in Czech: "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**");

(c) the Military Intelligence (in Czech: "Vojenské zpravodajství") for the purposes set out in Section 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 evidence 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.

Criminal Procedure Code

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 Act

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.

Military Intelligence Act

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 Sec. 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 6 months and is obliged to disclose such data (including metadata) to the following authorities on request:

(a) the police taking part in criminal proceedings, for the purposes and under the conditions prescribed by Sec. 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 Sec. 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 Sec. 8a of the Security Information Service Act;

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

(e) the Czech National Bank for the purposes and under the conditions prescribed by Sec. 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 Sec. 3 of the Decree No. 357/2012 Coll, on the preservation, transfer and deletion of traffic and location data"). In relation to the form and extent of the data, Sec. 97 of the Electronic Communications Act 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.

Criminal Procedure Code

Under Sec. 88a of the Criminal Procedure Code, the police of the Czech Republic 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.

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

Under Sec. 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 Force on request with information from its database of participants, to the extent and in the form prescribed by the Information Decree.

3. NATIONAL SECURITY AND EMERGENCY POWERS

Electronic Communications Act

Under Sec. 99 of the Electronic Communications Act, a legal entity providing a public communications network or a publicly-available electronic communications service (such as Vodafone) must provide priority access to the network for emergency communication participants (i.e. 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 the 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 Sec. 35(3) of the Act No. 341/2011 Coll., on the "**General Inspection of the Security Forces and Sec. 66(2) of the Police Act**".

Under Sec. 39(11) 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 to the necessary extent, the operator (provided that informing the operator will not jeopardise the police force's fulfilment of its duties).

Act No. 222/1999

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 further 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 Sec. 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 (i.e. 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 Sec. 88(3) of the Criminal Procedure Code, the police of the Czech Republic must continuously evaluate whether the issuance of the surveillance and recording order is still justified. If the grounds no longer exist, the police 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 Services Act

Under Sec. 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/she concludes that this is not the case.

Military Intelligence Act

Under Sec. 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/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.

Democratic Republic of Congo

In this report we provide an overview of some of the legal powers under the law of Democratic Republic of Congo ("DRC") that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

Framework Law No. 013-2002 of 16 October 2002 on tel-ecommunications

Articles 54(a) and 55 of the Framework Law No. 013-2002 of 16 October 2002 on telecommunications in the 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 DRC; or (iii) prevent crime and organized crime.

2. DISCLOSURE OF COMMUNICATIONS DATA

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

- 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 the 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.

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 can be applied. Article 4 of Decree-Law No. 1-6l of 25 February 1961 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

This 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 use of interception, the offence leading to the use of the interception and its duration (Article 56 of the Framework Law).

This authorization of the Minister of the Interior shall be given in writing and by justifiable decision. The authorization must be proposed by the Minister of Defence and security or proposed 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 DRC.

Egypt

In this report we provide an overview of some of the legal powers under the laws of Egypt that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

Constitution of Egypt

Article 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 (Law 58 of 1937) and the Criminal Procedures Code (Law 150 of 1950)

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 authorizing 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 misdemeanor 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 authorized member of the armed forces or security agencies. There are no explicit regulations regarding the latter.

The Communications Law (Law 10 of 2003)

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 (Law 150 of 1950)

The Egyptian Criminal Procedures Code 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 misdemeanor 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 authorized 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 (Law 58 of 1937) and the Criminal Procedures Code (Law 150 of 1950) requires 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.

Anyone claiming violation of privacy or illegal wiretapping can bring a 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.

Countries F-J

Fiji

In this report we provide an overview of some of the legal powers under the law of Fiji that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

Telecommunications Promulgation 2008

Under s.73(2) of the Telecommunications Promulgation 2008, mobile network operators must give officers and authorities of the government such help as is reasonably necessary for the purposes of enforcing criminal law and enforcing laws imposing pecuniary penalties, protecting public revenue and safeguarding national security. S.73(3) further states that mobile network operators will not be liable for an action or other proceedings for damages, if such act was committed in good faith (in accordance with s.73(2). The provisions of s.73(4) also provide identical indemnities to any director, officer, employee or agent of the mobile network operator.

In Fiji, there appear to be no specific laws that grant government law enforcement agencies the authority to have direct access into a mobile network operator's network without the operational control or oversight of the mobile network operator.

2. DISCLOSURE OF COMMUNICATIONS DATA

Telecommunications Promulgation 2008

Government agencies and law enforcement authorities may possess the legal powers under s.73 (2) of the Telecommunications Promulgation 2008 (Promulgation) to compel mobile network operators to disclose metadata.

Compulsory Registration of Customers for Telephone Services Decree 2010

The Compulsory Registration of Customers for Telephone Services Decree 2010 requires all providers of public mobile and fixed line telephone communications services (including any mobile virtual network operators) to obtain (and possibly retain for the period of 6 years) customer information.

Under s. 13 (1) of the Compulsory Registration of Customers for Telephone Services Decree 2010, a magistrate or justice of the peace (on reasonable suspicion or inquiry) may issue a warrant authorising a police officer to obtain customer registration details connected to one or more telephone numbers if the magistrate or justice of the peace thinks such information is necessary for investigations relating to prank calls to national emergency telephone numbers and also for investigations under the Crimes Decree 2009 relating to treason, offences against the government, offences against public order, offences against international order, offences against the person and threat of injury to a person employed in the public service.

Criminal Procedure Decree 2009

S.98(1) of the Criminal Procedure Decree 2009 permits a magistrate or justice of the peace (where proved in fact or on reasonable suspicion) to authorise a police officer or other person named in a search warrant to search any building, ship, carriage, box, receptacle or place named or described in a warrant. S. 98(2) permits the officer or any other person named in the warrant to seize the item and take it to the court issuing the warrant or some other court to be dealt with by the relevant law. In such instances the warrants may require the seizure of all electronic devices and any storage devices if such items are used or are reasonably believed to have been used in the commission of an offence.

Fiji Independent Commission Against Corruption

The Fiji Independent Commission Against Corruption Promulgation 2007 establishes the Fiji Independent Commission Against Corruption which is the body primarily responsible for investigating and prosecuting corruption in government and the public sector.

Under s. 10B of the Fiji Independent Commission Against Corruption Promulgation 2007, a magistrate who is satisfied on information on oath that in any premises or place where there is evidence of a commission of an offence the officer assisting the magistrate may enter upon and search the place or premises and seize any items which the officer believes may contain evidence of any offence.

3. NATIONAL SECURITY AND EMERGENCY POWERS

Except as already outlined this this report, the government does not have any other 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.

If a state of emergency is declared by the President under the Emergency Powers Act 1998, the President may on advice of the Cabinet make regulations affecting access to communications and/or networks.

Fiji has enacted a new Constitution in 2013. Under s.154 of the Constitution it is the Prime Minister, on advice of the Commissioner of Police and Commander of the Fiji Military Forces, who can declare a State of Emergency. The Constitution provisions therefore impliedly repeal the Emergency Powers Act.

4. OVERSIGHT OF THE USE OF POWERS

If a mobile network operator is required to provide assistance under the Telecommunications Promulgation 2008, it does on the basis that it neither profits from, nor bears the costs of, giving that help. Assistance is provided subject to terms and conditions agreed by the mobile network operator and the government; if no agreement is reached, these will be determined by an arbitrator appointed by the Telecommunications Authority of Fiji under s 74 of the Promulgation.

France

In this report we provide an overview of some of the legal powers under the law of the France that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

1. PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

French Criminal Procedure Code

The French Criminal procedure code (hereinafter the "CPP") provides 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 article 100 of the CPP, the judge's decision must be in writing and issued for maximum period of 4 months (renewable once under the same conditions of form and duration).

Article 706-95 of the CPP provides 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 detention") an authorisation to implement the interception, recording or 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 fifteen days, 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 one month (renewable once under the same conditions of form and duration).

The CPP provides 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.

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 98-7-III of the French Code of Post and Electronic Communications (hereinafter the "CPCE") also provides that electronic networks operators are under the 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.

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.

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 offense 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/she participated to the offense) 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 himself 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 the French customs (Article 65 of the Customs code).

3. NATIONAL SECURITY AND EMERGENCY POWERS

Code of National Security

Article L 244-2 of the CNS provides that the competent authorities can request from electronic communications network operators that they provide all necessary information relating to the implementation or exploitation of authorised interceptions.

Article L244-3 of the Code of National Security (in French the Code de la Sécurité Intérieure, created on 12 March 2012 by gathering a number of existing laws, hereinafter the "CNS") expressly provides 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 CNS and of the Code of Criminal Procedure (the "CPP").

Communications data may be required based on a standard request issued by intelligence agents sent to the relevant service provider. The request must in most cases have been authorised by the Prime Minister after a written and justified request sent by the Ministry of Homeland Security or by the Ministry of Defence or of the Ministry of Economy. Prime Minister authorisation is not necessary for access to documents and information necessary to conduct general surveillance of radio transmissions.

In addition, on 18 December 2013, the French parliament adopted a new law on military spending for the period of 2014 to 2019 in which modifications to the CNS were adopted. Among these, certain provisions have been added to the rules relating to government access to metadata which will come into force as of 1 January 2015.

According to future Articles 246-1 through to 246-5 of the CNS, duly appointed agents of the Ministries of Homeland Security, of Defence and of Economy will be entitled to request access to identification information from electronic communication services providers and internet service providers if justified by the purposes which may justify the authorisation of security interceptions by the Prime Minister. Agents of the intelligence services may request from all operators of electronic communications that they provide any information or documents "processed or retained by their networks or electronic communications services".

Such request is made further to a written authorisation issued by the Prime Minister which is valid during 30 days.

In addition, these provisions will also allow agents to request disclosure of the data in real time. The provision is intended, among other things, to permit intelligence agencies to have access to location data in real time.

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 provides 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 (e.g. 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 are not subject to judicial oversight.

Interceptions authorised by the Prime Minister on the basis of the CNS are subject to review by the Commission for the Control of Security Interceptions (hereinafter the "CCSI") which only has a consultative role and whose intervention only occurs after the decision of the Prime Minister. The Prime Minister is required to send his or her decision to the President of the CCSI within 2 days of the decision. If the President of the CCSI considers that the legal grounds of the decision are challengeable, he or she calls for a meeting of the CCSI which must issue its position within 7 days of receipt of the decision by its president. If it considers that the interception has been authorised in violation of the relevant legal provisions, the CCSI issues a recommendation to the Prime Minister, to the Minister who requested the interception and to the Minister in charge of Electronic Communications. The Prime Minister is not bound by the recommendation but is required to immediately advise the CCSI of the measures undertaken further to the recommendation. The CNCIS is informed afterwards but has no power to cancel or modify the request.

Germany

In this report we provide an overview of some of the legal powers under the law of Germany that government agencies have to order Vodafone's assistance with conducting real-time interception and disclosure of data about Vodafone's customers.

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 organizational capabilities to execute interception measures provided for by law (Sec. 110 TKG).

Sec. 110 TKG requires operators of telecommunication systems used to provide telecommunication services to the public (as further specified in Sec. 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 organizational 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 Sec. 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 (Sec. 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 Sec. 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 (Sec. 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 (Sec. 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 (Sec. 100b(3) StPO). The measures to be taken are further specified by Sec. 110 TKG and the TKÜV/TR-TKÜV.

Article 10 Act (Artikel 10-Gesetz-G10)

An order under Sec. 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 Sec. 3(1) G10) will be, is being, or has been committed, or 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 (Sec. 3(2) G10; "individual interception").

An order under Sec. 5 (for bundled telecommunications) or Sec. 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 with impact on German territory (as listed in Sec. 5(1) G10) or to prevent the danger to the life or physical integrity of a person abroad, if such danger directly affects German interests (Sec. 8 G10).

The interception measures under Sec. 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 (Sec. 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 (Sec. 110(1) No. 5 TKG and Sec. 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 equipment of the Federal Intelligence Service. The communication is filtered by this 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 (Sec. 2(1) G10). The measures to be taken are further specified by Sec. 110 TKG and the TKÜV/TR-TKÜV.

Customs Investigations Services Act ("ZFdG")

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

Federal Criminal Police Office Act ("BKAG")

Interception orders under Sec. 20l BKAG are granted via court order upon request by the President of Federal Criminal Police Office (Sec. 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 Sec. 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 (Sec. 20l(5) BKAG). The measures to be taken are further specified by Sec. 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, e.g., Sec. 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 Sec. 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 authorization (Sec. 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.

Code of Criminal Procedure

The Strafprozessordawng ("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 (Sec. 100g StPO). Similar powers as under Sec. 100g StPO are granted to the Customs Criminal Investigation Officer under Sec. 23g ZFdG, Federal Criminal Police Office under Sec. 20m BKAG, to the Federal Office for the Protection of the Constitution under Sec. 8a BVerfSchG, to the Military Counterintelligence Service under Sec. 4a MADG and the Federal Intelligence Service under Sec. 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 Sec. 100a StPO, Sec. 20l BKAG, Sec. 3 G10, Sec. 23a ZFdG and the respective provisions in the Police Acts of the federal states (see Sec. 5 and 7 TKÜV). Similar principles apply to measures under Sec. 5 and 8 G10 (Sec. 2(1) G10).

Subscriber Data, Line Identification and Other Data

Sec. 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 Sec. 95 and 111 TKG) to certain public authorities listed in Sec. 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 authorization. Respective authorizations (which may stipulate further requirements) are, for example, set out in Sec. 100j StPO, Sec. 7 and 15 ZFdG, Sec. 7, 20b and 22 BKAG, Sec. 22a BPolG, Sec. 8d BVerfSchG, Sec. 4b MADG and Sec. 2b BNDG.

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

Sec. 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 Sec. 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 Sec. 112(2) TKG). Sec. 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.

Traffic Data

Sec. 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 Sec. 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 (Sec. 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 (Sec. 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 (and certain the officials working in the police force or, in relation to tax offences, the tax authority) and to provide all necessary information without delay (Sec. 100g(2) and 100b(3) StPO).

Similar principles as under Sec. 100g StPO apply for information requests under

- Sec. 23g ZFdG and Sec. 20m BKAG, and
- Sec. 8a BVerfSchG, Sec. 4a MADG and Sec. 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 Sec. 100a StPO, Sec. 20l BKAG, Sec. 3 G10, Sec. 23a ZFdG and the respective provisions in the Police Acts of the federal states (see Sec. 5 and 7 TKÜV). Similar principles apply to measures under Sec. 5 and 8 G10 (Sec. 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 (Sec. 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.

Only where the content of customer communications is yet to be considered part of an on-going telecommunication process, then the content of the communication may only be accessed by means of an interception order according to Sec. 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 (Sec. 5(1) No. 3 TKÜV).

The request for disclosure under Sec. 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 Sec. 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 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 (Sec. 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.

4. OVERSIGHT OF THE USE OF POWERS

Code of Criminal Procedure ("StPO")

As well as what is set out above, according to Sec. 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 Sec. 98(2) or 304(2) StPO) against an interception order issued under Sec. 100a StPO, though it is recognized 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, i.e. no court order or warrant is required. However, the interception measures pursuant to Sec. 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 Sec. 3 G10 as long as such measure is not yet communicated to the person (Sec. 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 well-being of the federation or its states.

Customs Investigations Services Act (ZFdG)

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

Federal Criminal Police Office Act (BKAG)

The measures pursuant to Sec. 20l BKAG require a prior court order following an application by the President of Federal Criminal Police Office; yet, in pressing circumstances, the President of 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 (Sec. 20l(3) BKAG).

According to Sec. 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 Sec. 113 TKG, the judicial oversight and legal remedies depend on the specific different legal statutes granting the authorizations for the information requests.

For information requests pursuant to Sec. 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 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.

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

For information requests under Sec. 8d BVerfSchG, Sec. 4b MADG and Sec. 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 Sec. 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

As well as set above, according to Sec. 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 Sec. 98(2) or 304(2) StPO), though it is recognized that there is no legal obligation to verify or challenge the lawfulness of a request.

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

For information requests under Sec. 8a BVerfSchG, Sec. 4a MADG and Sec. 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 Sec. 100a StPO, Sec. 20l BKAG, Sec. 3, 5 and 8 G10, Sec. 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 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.

Ghana

In this report we provide an overview of some of the legal powers under the law of Ghana that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

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, provide any user information or otherwise in aid of law enforcement or national security.

Anti-Terrorism Act 2008

Pursuant 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 the 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 (L.I. 1991)

Regulation 103 of the Electronic Communications Regulations, 2011 (L.I. 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 communication 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, communication 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 provides 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 offer 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 law enforcement agency must first apply to the court and seek judicial approval before an order is granted relating to the disclosure of customers' communications that are in transit or held in electronic storage in an electronic communications system by a communication service provider. The court shall not make the order unless it is satisfied that the disclosure is relevant and necessary for investigative purposes or is in the interest 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").

Greece

In this report we provide an overview of some of the legal powers under the law of Greece that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

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 of the Hellenic Criminal Procedure Code.

The Hellenic Authority for Communications Security and Privacy ("**ADAE**") 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 (Decisions 52/2009 and 53/2009).

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.

Article 5(4) of Law 2225/1994 provides that an excerpt of the order, containing its operative part, is delivered to the Chairman, Board of Directors, General Manager or representative of the company concerned. According to Article 6(1) of Presidential Decree 47/2005, when a competent authority seeks the execution of an order, a service provider is obliged to activate the equipment and software required for the withdrawal of confidentiality within three hours from notification of the order, regardless of 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 the event of war, mobilisation due to external threats or an immediate threat to national security as well as 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 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.

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.

Article 5(4) of Law 2225/1994 provides that an excerpt of the order, containing its operative part, is delivered to the Chairman, Board of Directors, General Manager; or representative of the company concerned.

According to Article 7(2) of Presidential Decree 47/2005, the execution of an order for the withdrawal of confidentiality is performed by the competent authority in cooperation with the service provider.

3. NATIONAL SECURITY AND EMERGENCY POWERS

There are no additional powers, other than those set out above.

4. OVERSIGHT OF THE USE OF POWERS

Following the execution of an order, one or more reports are prepared by the service provider 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. The judicial authority that ordered the withdrawal of confidentiality may order its removal even before expiry of the time period set, if the purpose of the measure has been fulfilled or the reasons for its implementation no longer exist.

Hungary

In this report we provide an overview of some of the legal powers under the law of Hungary that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

National Security Service Act

Act CXXV of 1995 on the National Security Services (the "**National Security Service 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 Service 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, e.g. 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 Proceeding Act

Under section 202(6) of the Criminal Proceedings Act, interception by LEAs may only be conducted if obtaining evidence by other means reasonably appears to be 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 s.203 of the Criminal Proceedings Act, the competent court can issue an order for interception. Under sections 57-58 of 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 communication 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; e.g. a lockup room where the necessary equipment can be placed and non-stop technical assistance, if required.

Under section 3(3) and section 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 Communication 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, IMEI number, service use information, 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 (e.g. 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 Securities Act

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

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, 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 jeopardize 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 USE OF THE 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.

India

In this report we provide an overview of some of the legal powers under the law of India that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

Background

Indian Telegraph Act 1885 ("ITA")
This is the parent legislation governing telecommunications in India and the government grants the following licenses to service providers in accordance with the provisions of this Act:

Unified Access Service License ("UASL")
This is the license governing access service in India.

Internet Service Provider ("ISP") License
This is the license governing internet access service in India.

Unified License ("UL")
The Department of Telecommunications in 2013 issued the Unified License which is an umbrella license 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 license. Current UASL and ISP licensees will have to migrate to the Unified Licence Regime on expiry of their existing licenses. For the purposes of this report, we have relied upon the UASL and ISP licenses, 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 following rules:

(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.

(c) IT (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 ("Traffic Data Rules")

These Rules specify the procedure the government must follow to monitor and collect traffic data or information for the purposes of cyber security.

(d) IT (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 ("Blocking Rules")

These Rules specify the procedure the government must follow to order the blocking of IP addresses.

(e) IT ("Intermediaries Guidelines") Rules, 2011

These Rules specify the obligations of intermediaries to take down content under specified circumstances.

Code of Criminal Procedure, 1973
This is the principal law governing criminal procedure in India, and which authorises courts and law enforcement agencies to demand the production of documents or other information in the course of an investigation.

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

Legislation

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

The UASL and the ISP License 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 License 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 License the licensee is required to install the equipment that may be prescribed by the government for monitoring purposes.

3) As per Clause 34.28(xiv) of the ISP License and Clause 41.20 (xiv) of the UASL, in 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 License 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 as per Rule 3 of the Interception Rules, an officer not below the rank of the Additional Superintendent of Police shall 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'.

Licenses

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

Clause 41.10 of the UASL and Clause 34.6 of the ISP license provide that designated government officials shall have the right to monitor the telecommunication 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 License, 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 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 '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.

Licenses

Under the UASL and the ISP License Agreement, the licensee is required to provide access to all call data records as well 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 License 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 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 a summons or written order respectively, 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.

3. NATIONAL SECURITY AND EMERGENCY POWERS

Legislation

Under Section 5(1) of the ITA, if there is a public emergency or in the interest of public safety, 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.

Licenses

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

1) Under Clause 41.13 of UASL and Clause 10.5 of ISP License; 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 of India in the event of a national emergency, war, low-intensity conflict, or any other eventuality.

2) As per Clause 41.1 of UASL and Clause 34.1 of ISP License, 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 License, the government may revise the license 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 ISP License, 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 License 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 license, and will be considered an offence punishable under criminal law.

The ITA, the UASL and the ISP License 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 the central and the state level. As per 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 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.

Rule 419- A (17) provides that in case 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 7 working days, otherwise the interception will have to cease and the same message cannot be intercepted without the prior approval of 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.

Ireland

In this report we provide an overview of some of the legal powers under the law of the Republic of Ireland that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

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 Licenced 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 Licenced Operators to assist in implementing interception capabilities on their networks. However, for such a direction to authorise the implementation of interception capabilities on a Licenced 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 Licenced Operator's network (without the Licenced Operator's operational control or oversight).

In addition, section 2 of the 1993 Act provides 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 Licenced 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 interest 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 3 months, unless extended for a further 3 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 licenced under the 1983 Act ("**Licenced Operators**"). As Vodafone is a Licenced 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**)" provides 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 the purpose of 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).

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 Licenced Operator's network (without the Licenced 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 "**Licenced 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 which must be retained by Licenced Operators in relation to fixed network and mobile telephony, for two years:

(i) the names and addresses of subscribers or registered users;

(ii) the data necessary to identify the location of mobile communication equipment;

And including, in relation to internet access, internet e-mail and internet telephony, for one year:

(iii) the names and addresses of subscribers; and

(iv) 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 Licenced 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 produce to a member of an 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 powers, such as the power to put certain questions to persons present in 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 a Disclosure Order 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, e.g. 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 Licenced 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 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.

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, satisfy themself 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 Licenced 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.

Italy

In this report we provide an overview of some of the legal powers under the law of Italy that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

Real-time lawful interception forms part of the criminal investigation powers of the "law enforcement agencies" i.e. Police, Carabinieri, Tax Police and other authorised agencies: ("**LEAs**"), as authorised by the competent judge.

Italian Criminal Procedure Code

Interceptions within criminal proceedings (sections 266 to 271 of Italian Criminal Procedure Code): in proceedings related to certain crimes listed in section 266 (eg. bribery and corruption, crimes punished with imprisonment up to 5 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 and interception is necessary for the collection of evidence. In matters of urgency, the public prosecutor can directly authorise interceptions but the GIP shall make use of such authorisation within 72 hours. Interception orders are granted for 15 days, renewable for another 15 days (section 267 of the Italian Criminal Procedure Code). Real-time interceptions can be also authorised for electronic and telematics communications (section 266 of the Italian Criminal Procedure Code).

Implementing provisions of The Criminal Procedure Code

Preventive interceptions by LEAs (section 226 of Legislative Decree n. 271 of 1989): for the purpose of preventing crimes by criminal associations and international terrorism organisations, the Minister for Home Affairs or, where delegated by the latter, the Head of IT Department of an LEA or, in certain cases, the Head of Anti-Mafia Investigation Department, are entitled to ask the public prosecutor to authorise real-time interceptions. Interceptions orders are granted for 40 days, renewable for a further 20+20 days.

Legislative Decree n. 144 of 2005, as amended by Law n.133 of 2012

Preventive interceptions by intelligence agencies (section 4 of Legislative Decree n. 144 of 2005, as amended by Law n. 133 of 2012): the Prime Minister and, where delegated by the latter, the heads of Italian intelligence agencies (i.e. **AISE** and **AISI**) are entitled to ask the public prosecutor of Rome Court of Appeal to authorise interceptions for preventing crimes by criminal associations and international terrorism organisations or, more generally, in the interest of national security. The public prosecutor can authorise the requested interceptions through a reasoned decision. Interception orders are granted for 40 days renewable for further 20+20 days.

Given the legal framework described above, the relevant legislation regulating technical interception capabilities are the following:

Legislative Decree n. 259 of 2003 ("**Electronic Communications Code**") prescribes that communication service providers ("**CSPs**": i.e. Vodafone) shall comply with any order for interceptions issued by judicial authorities by agreeing with the LEAs over the terms and formalities of their performance.

On December 15, 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 a number of security measures with respect to mechanisms adopted by the CSPs for carrying out the interceptions.

Electronics Communication Code

As a general rule, section 96 of the Electronic Communications Code provides for the obligation of CSPs to render assistance and provide information to judicial authorities and LEAs in relation to interception operations for the purposes of justice and public security. Pending the adoption of the Repertorio provided for by article 96 (2) (i.e. a detailed catalogue of mandatory interception services and technical standards which has never been formally adopted although a draft of it is accessible by telecom operators) technical capabilities are from time to time agreed between the CSPs and public prosecutor/LEAs.

Italian Privacy Authority's Guidelines

The Italian Privacy Authority's Guidelines of December 15, 2005 oblige CSPs 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:

1) 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 characteristics.
2) Security of the information data flows with the judiciary authority:
   - use of communication 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.
3) Protection of data processed for justice purposes:
   - 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; 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.

Interception operations are normally carried out not directly by Vodafone but through equipment installed at the requesting authorities office (or at an interception centre indicated by the requesting authority). However, in case of interception of "telematic" communications, the public prosecutor may order that the relevant interceptions be carried out also through equipment owned by private entities or individuals (section 268 (3) of Italian Criminal Procedure Code).

According to section 11 of the Prime Minister Decree of January 24, 2013, CSPs, such as Vodafone, providing electronic communication networks or services can be required, among other things, to allow intelligence agencies (AISE and AISI) and the National Security Department ("**DIS**") to access their databases on the basis of specific agreements setting out the modalities of such access.

2. DISCLOSURE OF COMMUNICATIONS DATA

According to article 13 (1) of Law no. 124 of 2007 on the reorganisation of the intelligence agencies, CSPs can be required to cooperate with intelligence agencies, disclosing to them information, including communications data relating to customer communications. This obligation has been recently clarified in section 11 of the Prime Minister Decree of January 24, 2013 which directly refers to the mentioned Law no. 124 of 2007. This states that CSPs are required to "provide information" to intelligence agencies (AISE and AISI) and the National Security Department (DIS) according to their respective competences as set out by Law 124 of 2007, on the basis of specific operational agreements, in the interest of national security: i.e. in order to protect the independence, integrity and security of the Republic from any internal or external subversive activity and criminal or terrorist attack:

Moreover, according to the relevant provisions of the Italian Criminal Procedure Code and Legislative Decree n. 271 of 1989, CSPs can be required to provide LEAs (duly authorised by the judicial authority) with metadata relating to customers communications within criminal proceedings as follows:

a) **Seizure of data in the possession of CSPs within criminal proceedings** (section 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; and

b) **Access to customers' data by LEAs** (section 226 (4) of Legislative Decree n. 271 of 1989): for the purpose of preventing crimes by criminal associations and international terrorism organisations, the Minister for Home Affairs or, where delegated by the latter, the LEAs' Head of IT Department or, in certain cases, the Head of Anti-Mafia Investigation Department are entitled to ask the public prosecutor to order CSPs to trace telephonic and telematic communications and to authorise access to data relating to such communications and to any other relevant information stored by CSPs.

In addition, section 55 of the Electronic Communications Code sets forth the obligation for CSPs to provide the Minister of Home Affairs with a list of all their customers or purchasers of pre-paid mobile traffic.

Moreover, according to the relevant provisions of the Italian Criminal Procedure Code and Legislative Decree n. 271 of 1989, CSPs can be required to provide LEAs (duly authorised by the judicial authority) with customers' content data stored in their database.

3. NATIONAL SECURITY AND EMERGENCY POWERS

There are a number of provisions allowing the government to dispose of networks in times of emergencies, such as:

a) Section 13 (1) of Law no. 124 of 2007, as clarified by section 11 of Ministerial Decree of January, 24 2013;

b) Section 73 of the Electronic Communication Code;

c) Section 2 of T.U.L.P.S. (Reformed Law on Public Security).

Section 2 of Law no. 225 of 1992 on the Civil Protection service provides that CSPs must cooperate with the management of a cyber crisis, contributing to help restore network and communication system functionalities.

Section 73 of the Electronic Communication Code establishes that, in case of severe network crash, force majeure or natural disaster, the Ministry of Communications is entitled to set forth the measures needed for guaranteeing the availability of the public phone network. CSPs must implement all the necessary measures for guaranteeing non-stop access to emergency services.

According to Section 2 of T.U.L.P.S. (Reformed Law on Public Security) the Prefect, in case of urgency or state of necessity, is entitled to adopt all the necessary decisions for protecting public order and public security.

Pursuant to Section 2 of Law no. 225 of 1992, 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 what is set out above, Section 96(2) and Section 32 of the Electronic Communications Code set out sanctions for those CSPs which do not comply with specific obligations to cooperate with judicial authorities and law enforcement agencies in relation to interception operations.

The judiciary plays no role in the execution of the operational agreements between the intelligence agencies and the CSP, or in the access operations. However, such agreements are notified to the COPASIR (a special Parliament Committee which controls Italian intelligence activities) and the latter is annually informed on the number of accesses to such these databases.

In case of seizure carried out within criminal proceedings the authorisation and control of the GIP is necessary on the basis of the public prosecutors' request.

In case of access to customers' data by LEAs, the authorisation and control of the competent public prosecutor is necessary.

The activity of the Intelligence agencies is directly monitored by the Prime Minister and by COPASIR, whose function is to systematically ensure that the agencies operate in compliance with the Constitution and the law.

Countries K-O

Kenya

In this report we provide an overview of some of the legal powers under the law of Kenya that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

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) ("NIS Act") allows the Director-General of the National Intelligence Service ("NIS") (pursuant to Section 36) to monitor or otherwise interfere with the privacy of a person's communications.

Pursuant to Section 42 (1) and (2) of the NIS Act, where the Director-General has reasonable grounds to believe that a warrant under this section is required to enable the NIS to investigate any threat to national security or to perform any of its functions, he or she may apply for a warrant. Section 42 (2) of the NIS Act provides that such a warrant shall be ex-parte before a judge of the High Court of Kenya.

The Director-General of the NIS can apply for a warrant (issued by the High Court of Kenya pursuant to Section 36 of the NIS Act) that enables investigations of a person's private communications. Further, Section 44 of the NIS Act allows the Director-General of the NIS to request the courts to direct the appropriate persons to furnish such information, facilities or technical assistance as necessary to execute the warrant.

Section 45 of the NIS Act provides that, a warrant issued under the Act may authorise any member of the NIS to obtain any information, material, record, document or thing and for that purpose:

(a) to enter any place, or obtain access to anything;

(b) to 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 things;

(c) to monitor communication; or

(d) to install, maintain or remove anything.

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 specified communication of a specified description received or transmitted or about to be received or transmitted by the communications service provider or authorising 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 Mutual Legal Assistance Act (Cap. 75A Laws of Kenya)

Pursuant to The Mutual Legal Assistance Act (Cap. 75A Laws of Kenya) (the "MLA Act") a requesting state may make a request to Kenya requesting 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 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 provides that a request may be made to Kenya from a requesting state for deployment of covert electronic surveillance.

Kenya Information and Communications Act (Cap. 411A, Laws of Kenya)

The statutes mentioned above should be considered in the context of Section 31 of the Kenya Information and Communications Act (Cap. 411A, Laws of Kenya) (the "KIC Act ") which makes it an offence punishable by conviction with a fine not exceeding three hundred thousand shillings, or imprisonment for a term not exceeding three years, or to both where a licensed telecommunication operator who otherwise than in the course of his business:

- intercepts a message sent through a licensed telecommunication system; or
- discloses to any person the contents of a message intercepted; or

- discloses to any person the contents of any statement or account specifying the telecommunication services.

Section 93 of the KIC Act has the effect of obliging a person licensed to provide telecommunication services to disclose information (interception being a mode of disclosure) where such disclosure facilitates the statutory functions of the Commission or is in connection with the investigation of a criminal offence or to facilitate criminal proceedings or for the purposes of any civil proceedings brought by virtue or/under the KIC Act.

Kenya Information and Communications (Consumer Protection) Regulations, 2010

Further, Regulation 15 (1) of the Kenya Information and Communications (Consumer Protection) Regulations, 2010 require that, subject to the provisions of the KIC Act or any other written law, a licensee (licensed under the KIC Act) shall 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 are however qualified by Section 93 of the KIC Act which allows for disclosure of information where such disclosure facilitates the statutory functions of the Commission or is in connection with the investigation of a criminal offence or to facilitate criminal proceedings or for the purposes of any civil proceedings brought by virtue of/under the KIC Act.

2. DISCLOSURE OF COMMUNICATIONS DATA

Kenya Information and Communications Act (Cap. 411A, Laws of Kenya) ("KIC Act")

Section 89 (1) of the KIC Act provides the power 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, test any station or apparatus or obtain any article or thing.

The National Intelligence Service Act (Act No. 28 of 2012) ("NIS Act")

Section 44 of the NIS Act allows the Director-General of the NIS to request the courts to direct the appropriate persons to furnish such information, facilities or technical assistance as necessary to execute the warrant. Section 45 of the NIS Act provides that a warrant issued under the Act may authorise any member of the NIS to obtain any information, material, record, document or thing.

The Mutual Legal Assistance Act (Cap. 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 (Cap 59B)

Section 103 of the Proceeds of Crime and Anti-money laundering Act (Cap.59 B) 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 the 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 AND EMERGENCY POWERS

The National Intelligence Service Act (Act No. 28 of 2012) ("NIS Act")

As described above, pursuant to section 42 (1) and (2) of the NIS Act where the Director-General has reasonable grounds to believe that a warrant under this section is required to enable the NIS to investigate any threat to national security or to perform any of its functions, he or she may apply for a warrant before a Judge of the High Court of Kenya (under section 36) to monitor or otherwise interfere with the privacy of a person's communications to enable investigation of any threat to national security.

The Constitution of Kenya 2010

Under Article 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 fourteen days from the date of declaration, unless the National Assembly resolves to extend the declaration. After 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.

4. OVERSIGHT OF THE USE OF POWERS

The role of the judiciary pursuant to the NIS Act is limited to issuing the warrant and any subsequent judicial orders (related to the warrant). However pursuant to Section 45 of the NIS Act, in extreme cases of emergency, the Director-General may exercise the powers under the NIS Act without a warrant provided that he applies for a warrant within thirty six hours after exercising any of the powers under the NIS Act.

Further, Section 65 of the NIS Act provides that 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 declaration of a state of emergency and any legislation enacted, or other action taken, in consequence of a declaration of a state of emergency.

Lesotho

In this report we provide an overview of some of the legal powers under the law of Lesotho that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

Communications Act 2012

Section 44(1)(f) of the Communications Act 2012 ("**Communications Act**") provides 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 of 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 provide 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/she believes that by first obtaining the warrant it 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 provides 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 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 to among other things 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 consequences of that action.

Section 9 of the Ombudsman Act 1996 provides that in the performance of his functions the Ombudsman shall 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 provides that "The Minister may, on an application made by a member of or above the rank of Higher Intelligence Officer, issue a warrant authorizing 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 reasonable obtained by any other means".

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 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.

S. 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 authorized its issue and a statement of that fact is endorsed on it, it is signed by the Director General or an office authorized 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 (amongst other things) so requires. Therefore, laws of general application that limits 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/public order).

Malta

In this report we provide an overview of some of the legal powers under the law of Malta that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

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 provides that the function of the Security Service shall be to protect national security; in particular, against threats from organised crime, espionage, terrorism and sabotage, 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 shall 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 being a Permanent Secretary or the Cabinet Secretary.

Warrants are generally valid for six months (if issued by the hand of the Minister) or two days (if not issued under the hand of 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 ("**S.L.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 SL399.28 provides that the Malta Communications Authority shall 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 shall give reasons for the technical and operational requirements it defines and shall 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, whilst 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 ("**S.L.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.

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:

(i) the calling telephone number;

(ii) the name and address of the subscriber or registered user;

(b) concerning Internet access, Internet e-mail and Internet telephony:

(i) the user ID allocated;

(ii) the used ID telephone number allocated to any communication entering the public telephone network; and

(iii) the name and address of the subscriber or registered user to whom an Internet-Protocol 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:

(i) 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

(ii) the name and address of the subscriber or registered user;

(b) concerning Internet e-mail and Internet telephony:

(i) the user ID or telephone number of the intended recipient of an Internet telephony call; and

(ii) 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 e-mail and Internet telephony:

(i) 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 Internet Protocol 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

(ii) the date and time of the log-in and log-off of the Internet e-mail 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 e-mail 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:

(i) the calling and called telephone numbers;

(ii) the International Mobile Subscriber Identity of the calling party;

(iii) the International Mobile Equipment Identity of the calling party;

(iv) the International Mobile Subscriber Identity of the called party;

(v) the International Mobile Equipment Identity of the called party;

(vi) 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 services was activated;

(c) concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone numbers for dial-up access; and

(ii) 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 location label (Cell ID) at the start of the communication; and

(b) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

Pursuant 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 purpose of the investigation, detection or prosecution of a serious crime.

SL440.01 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 SL440.01 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 shall be "clear and specific", provided that where the data is urgently required, such request may be made orally, however a written version of the request shall be made at the earliest opportunity.

Regulation 18(1) of SL440.01 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.

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 him.

If information is provided pursuant to 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 so attends at the police station or place indicated to him he shall be deemed to have attended that police station or other place voluntarily. The written notice shall contain a warning of the consequences of failure to comply, namely that such person shall be guilty of a contravention punishable with detention and shall 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 in accordance with the advice of the Prime Minister, may, subject to the provisions of the Constitution of Malta, make such regulations as appear to him 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. Such regulations (in accordance with Article 4(2) of Chapter 178) can include authorising the 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 shall 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 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 shall keep under review, among other things, the exercise by the Minister responsible for the Security Service of his powers to issue warrants.

The Information and Data Protection Commissioner is responsible for the compliance and enforcement of SL440.01. 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.

Mozambique

In this report we provide an overview of some of the legal powers under the law of Mozambique that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

Decree n.º33/2001

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 n.º33/2001**" of 6th of 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 shall be made through the Regulatory Authority's duly credentialed members. The law does not appear to provide a clear outline of the process; neither is there a law or decree that establishes such procedures.

In Mozambique, there appear to be no specific laws that grant government agencies the legal powers to permit direct access into a telecommunications operator's network without the operational control or oversight of the telecommunication operator.

2. DISCLOSURE OF COMMUNICATIONS DATA

The Telecommunications Law

Article 68 of the Telecommunications Law (Law n.º8/2004 of 21st of July – the "**Telecommunications Law**") states that secrecy of the communications is guaranteed except in cases of criminal law and in cases of interest to national safety and the prevention of terrorism, criminality and organised delinquency.

3. NATIONAL SECURITY AND EMERGENCY POWERS

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

Article 10 of the Telecommunication 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; neither 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.

The Netherlands

In this report we provide an overview of some of the legal powers under the law of The Netherlands that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

Telecommunications Act

Pursuant to Article 13.1 of the Telecommunications Act ("**TCA**") providers of public telecommunications networks and publicly available telecommunications services ("**service providers**") shall only make their telecommunications networks and telecommunications services available to users if these can be wiretapped. Rules may be set by or pursuant to a general administrative order regarding the technical susceptibility to tapping of public telecommunications networks and publicly available telecommunications services.

The TCA requires public telecommunication service providers to set up and maintain a reasonable interception capability in its network. This includes the capability for the service provider in question to be able to implement an interception after having received an interception warrant.

It should be noted that the service provider shall 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 pursuant to the Dutch Code of Criminal Procedure ("Wetboek van Strafvordering" or "**DCCP**") or consent pursuant to the Intelligence and Security Services Act 2002 ("Wet op de inlichtingen- en veiligheidsdiensten 2002" or "**ISSA**") for 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 give effect to 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 intercept warrant where the public prosecutor believes it is necessary in the interests of investigation of criminal cases.

The Minister of Interior and Kingdom Relations may furthermore authorise interception by the General Intelligence and Security Agency ("Algemene Inlichtingen- en Veiligheidsdienst" or "**AIVD**") and the Minister of defence may authorise interception by the Military Intelligence and Security Agency ("Militaire Inlichtingen- en Veiligheidsdienst" or "**MIVD**") pursuant 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 unauthorised interception is a criminal offence (Article 139c DCC) which can lead to a penalty of maximum EUR 20.250.

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 TCA states that the service provider is obliged to provide the data requested on the basis of articles 126(n), 126(na), 126(u), 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 ISSA. The ISSA also provides for an obligation to cooperate in decrypting the data.

The service provider is obliged to retain and/or provide location data and traffic data and data which can identify the user of the telecommunications network (article 13.2(a) TCA and articles 126(ng), 126(ug) and 126(zh) DCCP. Generally, the content of customer communications is not stored. However articles 126(ng), 126(ud) and 126(ug) DCCP provide 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 decrypting the data (article 126(nh) and 126(uh) DCCP).

Article 13.2(a) TCA states that the service provider is obliged to retain certain information. Pursuant to article 13.2(b) 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) DCCP to disclose such information to the law enforcement agency.

3. NATIONAL SECURITY AND EMERGENCY POWERS

In exceptional circumstances connected with the enforcement of international rules of law or 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 telecommunication 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 TCA)

In addition, under article 14.4 of the TCA (which has not yet entered into force) the Minister of Economic Affairs, shall be empowered, in the event of exceptional circumstances that make this necessary, to give instructions to service providers in relation to – amongst other things – the maintenance, exploitation or use of their public telecommunications networks. In case of a war, the Minister of Economic Affairs may only do so in agreement with the Minister of Defence (Article 14.3 TCA). Pursuant to article 14.2 TCA, Article 14.4 TCA may only enter into force by Royal Decree, on the recommendation of the Prime Minister.

4. OVERSIGHT OF THE USE OF POWERS

Instructions given by the Minister cannot be appealed and authorisation of a supervisory-judge must be obtained in respect of the investigations of criminal cases.

New Zealand

In this report we provide an overview of some of the legal powers under the law of New Zealand that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

Background

The information outlined below represents the law as in effect from 11 May 2014. This is when the Telecommunications (Interception Capability) Act 2004 (TICA) is 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 March 2014) are based on the to-be-repealed TICA. Accordingly, the Guidelines (as updated from time to time) may be replaced or removed under the new TICSA (which will be in force in full from 11 May 2014).

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

The Telecommunications (Interception Capability and Security) Act 2013

The Telecommunications (Interception Capability and Security) Act 2013 (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 (GSCB Act);
- the Search and Surveillance Act 2012 (SAS Act); and
- the New Zealand Security Intelligence Service Act 1969 (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;
  - to 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.

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 operators 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 (i.e. the provision of a physical medium, such as optical fibre cable, over which telecommunications are transmitted); or
- any wholesale network service it provides (i.e. 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 which 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:

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 cyber security 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 thing 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

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.

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 the enforcement officer has intercepted (see section 55(3)(g) of the SAS Act) (i.e. if the content of the telecommunications had 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 the stored content of telecommunications. A network operator would then, in being requiring 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 an 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
- 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).

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.

International Terrorism (Emergency Powers) Act 1987

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 a 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 in the situation of being 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 s/he is satisfied that the proposed interception is for the purpose of cyber security 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 (i.e. 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 well-being 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.

Countries P-S

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.

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

The Constitution of the Portuguese Republic

There are two instances in which the Portuguese courts can authorise and demand the provision of real-time interception assistance:

1. As per 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 under responsibility of the Government but of the Public Prosecutor jointly with a criminal judge; and
2. Articles 19, 134 and 138 of the Constitution for the Portuguese Republic, as well as law nr. 44/86, dated 30th of September (Legal Framework for the State of Siege and Emergency) permits 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 state of emergency has been decreed by the President of the Republic and approved by the Portuguese Parliament . The state of siege or state of 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 communication service provider to assist in intercepting customer communications provided that has been foreseen in the state of siege or state of emergency decree that the fundamental rights of article 34 of Constitution of the Portuguese Republic are suspended. Nevertheless the government order should be communicate 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 of the Portuguese Republic and would be punishable as a crime.

Portuguese Criminal Proceedings Code

For the interception of communications in the context of a criminal proceeding the rules established in articles 187–190 of the Portuguese Criminal Proceedings Code, interception may only be authorised in case 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 3 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) organized 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 nr. 9/2007, dated 19th February 2007, 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 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 nr. 53/2008

Law nr. 53/2008, dated 29th August 2008, establishes the legal provisions applicable to Homeland Security in Portugal. This Law outlines that access and control of communications may only be carried out following a judicial authorisation and solely performed by the police.

Portuguese Electronic Communications Law

Under article 27/o' of the Portuguese Electronic Communications Law (Law 5/2004, dated 10th February) and the operating licences granted to communication service providers, it is an obligation on the providers of electronic communications services and networks, to provide, at their own expense, systems for legal interception by competent national authorities, as well as supplying 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 (notably in 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 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 nr. 67/98 of 26 October (Portuguese Data Protection Act) and Law nr. 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 regime set out above for provision of real-time lawful interception assistance, namely in the context of a criminal proceeding, and provided that a judicial authorization has been sought and the rules established in articles 189–190 of the Portuguese Criminal Proceedings Code are followed. However, in case the state of siege or state of emergency has been decreed the exceptional regime 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 30/84 of 5 of September, it is not allowed to pursue actions that may constitute an offence to the fundamental rights, liberties and guarantees as set out in the Portuguese Constitution and Law.

Additionally, this law also establishes that the agency does not have powers to pursue any type of acts that are in the scope of the courts and police authorities' competence.

In the event of the suspicion 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, in that case, if relevant to the investigation, the Public prosecutor may request to a Judge the gathering of evidence (e.g. through real-time interception or disclosure of metadata) according to the regime described above.

Constitution for the Portuguese Republic

Articles 19, 134 and 138 of the Constitution for the Portuguese Republic, as well as law nr. 44/86, dated 30th of 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 state of 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 state of emergency decree shall expressly determine which rights, liberties and guarantees shall be suspended.

The state of siege or emergency would only be effective upon specific enforcement by the President. These powers are absolutely 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 absolutely 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.

Qatar

In this report we provide an overview of some of the legal powers under the law of Qatar that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

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 Telecommunication Law (the "Telecommunication Law") and No. (1) of 2009 on the promulgation of the Executive By-Laws for the Telecommunications Law (the "Telecoms By-Laws") require operators of telecommunication systems used to provide telecommunication services to the public to intercept communications in real-time.

Article 59 of the Telecommunication Law states "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 interested in "State security" can rely on Article 59 of the Telecommunication Law alongside using any enforcement powers vested directly in the concerned government authority.

Article 93 of the Telecoms By-Laws states "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 the 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 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 cases, 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 communication service providers 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 involving national security and general emergency cases, the Qatari government agencies and law enforcement agencies can directly approach communication service providers to access their customer's communications data and/or network.

4. OVERSIGHT OF THE USE OF POWERS

There is no judicial oversight of the use 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 pursuant to the agreement with the Chairman of the Board of ictQATAR shall seize and prosecute offences committed in violation of the rules of the Telecommunications Law.

Romania

In this report we provide an overview of some of the legal powers under the law of Romania that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

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 per the applicable statutory provisions, unless parties to the communication consent in writing.

Interceptions may be made upon the request of intelligence and security agencies made under Article 123 of Law 51/1991 on regarding Romania's national security, i.e. where there are threats to the national security.

Decision no. 987/2012

Pursuant to Article 3.8 of Decision no. 987/2012 of the National Authority for Management and Regulation in Communications ("**ANCOM**") on the general authorisation regime for the provision of electronic communications networks and services, service providers must set up at their own cost the necessary technical means and take all other necessary technical measures required to immediately enforce the lawful authorisations or warrants issued for the interception of communications.

Criminal Procedure Code

The following rules under Article 139(1) of the Criminal Procedure Code (Law no. 135/2010), apply in relation to prosecuting certain categories of crime: (a) the measure taken is proportionate to the restriction of the rights and freedoms that it entails; and (b) 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 6 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).

Pursuant to the 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

As per Article 3.8. of ANCOM Decision no. 987/2012 (the "**ANCOM Decision**") on the general authorisation regime 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;

(ii) duly cooperate with the relevant authorities involved in interceptions;

(iii) cooperate with the relevant authorities to implement security and audit criteria of national communications interception system developed by them;

(iv) take all necessary technical measures to enable interceptions in general and immediately enable the enforcement 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.

As per Article 8(2)(k) of the Government Emergency Ordinance 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

Law 82/2012

Under Article 16 of Law 82/2012 on the retention of data generated and processed by providers of electronic communications, network service providers are to disclose any metadata retained in accordance with Law 82/2012 (i.e. the data necessary to (i) trace and identify the source of a communication, (ii) identify the destination of a communication, (iii) identify the date, time and duration of communication, (iv) identify the type of communication, (v) identify users' communication equipment or what purports to be their equipment; and (vi) identify the location of mobile communication equipment) within 48 hours of the request of the prosecutor's office, the courts of law or the national security authorities.

According to Article 12(1) of Law 82/2012 on Romania's national security, national security authorities may request retained data from telecommunication networks and service providers in case of threats to national security.

Criminal Procedure Code

As per Article 152(1) of the Criminal Procedure Code (Law 135/2010), the disclosure of metadata upon the Prosecutor's office request (i.e. where there are suspicions regarding the perpetration of certain crimes set out by Law 82/2012) needs to be authorised by a court decision following a request of the relevant prosecutor's office.

Under Article 138 of the Criminal Procedure Code (Law no. 135/2010), criminal prosecution bodies may access any computer systems in order to identify evidence, where:

(i) there is a reasonable suspicion about a serious offence/ crime;

(ii) the measure is proportional with 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.

Pursuant to Article 139(1) of the Criminal Procedure Code (Law 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).

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 them in court if they are necessary for the settlement of the case.

Under Article 19 of Council of Europe Convention on Cybercrime (E.T.S. No. 185, 23 November 2001) ratified by Romania under Law 64/2004, each party to the Convention is to adopt such legislative and other measures as may be necessary to empower its relevant authorities to search or access a computer system or a part of it and computer data stored therein, and any computer storage support that stores computer data on its territory.

3. NATIONAL SECURITY AND EMERGENCY POWERS

There are no express provisions regulating instruments used in the case of disclosure upon request of national security authorities. From Article 12(1) read in conjunction with Article 12(2) of Law no. 51/1991 in relation to Romania's national security, it may be inferred that, unlike in the case of interceptions which require a warrant granted by the court, disclosure of geo-location data can be made upon simple request of national security authorities.

Except as set out above, the government does not have the 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.

Under Article 1 and 3(c) of Law 132/1997 on requisitions, under exceptional circumstances (e.g. war, national emergency, disasters, etc.) public authorities and national defence forces can take temporary possession of any goods in order to gain access and use of the telecommunication systems.

As per Law 132/1997 on requisitions, the following instruments are required in view of a requisition of telecommunication networks assets:

(i) a requisition plan drawn up by the local authorities before the relevant events occur (Article 5(1)); and

(ii) a military order for hand-over to be issued at the date of the actual requisition (Article 14).

According to Article 18 of Government Emergency Ordinance 34/2008 on National System for Emergency Calls, the providers of electronic communications are obliged to make available to the director of the National System for Emergency Calls an updated database with all telephone numbers, names and address of customers that have placed emergency calls.

According to Article 20 of Government Emergency Ordinance no. 1/1999 during a state of siege or emergency, exceptional measures established by military authorities are enforced via military orders that are mandatory throughout the country.

4. OVERSIGHT OF THE USE OF POWERS

Other than what is set out above, there are the following rules relating 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 quantum of the compensation.

South Africa

In this report we provide an overview of some of the legal powers under the law of South Africa that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

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) prescribes 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 above activity was also a party to those communications;
- intercepting, monitoring or disseminating information of an employee while carrying on a business;
- interception to prevent serious bodily harm;
- interception to determine a location during an emergency; or
- when entitled to do so in terms of other legislation.

An interception direction can only be issued in the event that a judge is satisfied that a serious offence has been or will be committed, or the gathering of information is necessary concerning an actual threat to the 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 provides 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 the 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 provides that a telecommunication service provider must provide a telecommunication service which has the capability to be intercepted and store communication-related information. A directive prescribes the:

(i) capacity needed for interception purposes;

(ii) technical requirements of the systems to be used;

(iii) connectivity with interception centres;

(iv) manner of routing duplicate signals of indirect communications to designated interception centres; and

(v) manner of routing real-time or archived communication-related information to designated interception centres.

2. DISCLOSURE OF COMMUNICATIONS DATA

RICA requires a telecommunication service provider to intercept and stores 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 same.

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 judge of a High Court, a regional court magistrate or a magistrate for the issuing of same.

3. NATIONAL SECURITY AND EMERGENCY POWERS

Except as set out above, the South African government does not have any other 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.

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 the case may be. The "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 purposes of the act.

In respect of the maintenance of interception capability as required under Section 30 RICA, there is no judicial oversight of the requirements 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 telecommunication service provider/s concerned, must, on the date of the issuing of a telecommunication service licence, issue a directive as detailed directly above.

Spain

In this report, we provide an overview of some of the legal powers under the laws of Spain that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

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) Following the judicial police's initiative, a judge may issue an interception order following the legal requirements established in Article 579 of the Criminal Procedure Act, approved by Royal Decree of 14 September 1882 (the "**Criminal Procedure Act**"), in cases where evidence suggests that by making use of these means a relevant issue or circumstance of the case may be discovered or ascertained.

Organic Law 2/2002

(b) In addition, pursuant to the Organic Law 2/2002, dated May 6, 2002, on the Prior Judicial Control applicable to the National Intelligence Centre, the National Intelligence Centre ("**CNI**") may ask the operator to intercept communications in cases where the Secretary of State or Director of the CNI has obtained an authorisation from the relevant judge of the Spanish Supreme Court, in accordance with the aforementioned requirements of such Organic law.

(c) In cases of urgency, when investigations are carried out to find out felonies which are related with the acts of armed gangs, terrorist elements or rebels, the interception of communications may be ordered by the Minister of Home Affairs, or otherwise, the Director of State Security, communicating it immediately by a reasoned opinion in writing to the relevant judge, who will also by a reasoned opinion, revoke or confirm such resolution in a maximum term of 72 hours within 72 hours of being ordered.

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 2005 (the "**Universal Service Regulation**"), determines the procedure and the measures to be adopted by service providers and operators of public electronic communication networks for intercepting 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, interfaces, etc.).

In addition, Order ITC/110/2009, of 28 January 2009 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 in order to be communicated by the relevant agent about the need to carry out the interception of a communication.

A court order or an authorisation must be issued by the relevant judge before the interception takes place, except as outlined in case (c) above.

Order ITC/110/2009

Additionally, the relevant technical requirements and interfaces which service providers and operators of public electronic communication networks are required to have implemented to carry out the interception of a communication are regulated under Order ITC/110/2009, of 28 January 2009, on the general framework applicable to the specifications to be followed for the legal interception of communications.

General Telecommunications Act 32/2003

Article 33 of the General Telecommunications Act 32/2003, of 3 November 2003, sets out the operator's duty to intercept communications when required to do so by the relevant authorities through the appropriate interfaces, duly ready for this purpose. Together with such Act, the Universal Service Regulation and the General Framework Order, all provide for a detailed description of the obligations to which operators are subject 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: (1) the Order ITC/313/2010, 12 February 2010, implementing and adapting the technical specification ETSI TS 101 671 on Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic; (2) Order ITC/682/2010, dated March 9th, 2010, implementing and adapting the technical specification ETSI TS 133 108 (3GPP TS 33.108) on Universal Mobile Telecommunications System (UMTS); 3G security; and Handover interface for Lawful Interception (LI).

Spanish law does not appear to grant government agencies the legal powers to mandate direct access into a communication service provider's networks without the operational or control or oversight of the communication service provider.

2. DISCLOSURE OF COMMUNICATIONS DATA

Data Retention Act 2007

The Act 25/2007, of 18 October 2007, of retention of data related with electronic communications and public communication networks ("**Data Retention Act**"), regulates: (1) the operator's obligation to retain traffic and localisation data, and other necessary data to identify the user ("**traffic data**") generated or processed in connection with the provision of electronic communication services or public communication networks; and (2) 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 particular traffic data to be retained, the particular obligation to store traffic data, the period of time such traffic data must be stored or retained by the operator, the procedure and security measures involved in the transfer of such traffic data to the relevant agents, and the sanctions to be imposed on operators which do not comply with such obligations.

The content of communications is explicitly excluded from the scope of the aforementioned Act.

In accordance with Article 4 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 pursuant to the provisions of to the Criminal Procedure Act.

Article 8.2 of Law 34/2002 on Information Society Services and Electronic Commerce ("**LSSI**") states that in order for the competent authorities to identify an alleged infringer, they may request information society service providers (which may include telecoms operators) to disclose data which would permit such identification. This request has to be based on a previous judicial authorisation, in accordance with Article 122 of the Law 29/1998 of 13 July governing Administrative Jurisdiction ("**LJCA**").

3. NATIONAL SECURITY AND EMERGENCY POWERS

According to Article 4.5 of the General Communications Act, the Spanish Government may, exceptionally and temporarily, determine the assumption by the General Administration of the direct management of certain services or the exploitation of certain electronic communications networks, in order to ensure public safety and national defense.

According to the exceptional regime provided by Organic Law 4/1981 of 1 June, on the State of Alarm, Emergency and Siege ("**LSAES**"):

(a) during the State of Alarm (on the basis of essential goods stock-outs in the whole national territory or in a certain region – Article 4.d), the government may issue necessary orders (Article 11.e) or decide to intervene in such services or mobilize its personnel (Article 12.2) in order to insure the functioning of affected services;

(b) during the State of Emergency (which may be requested on the basis of serious alteration of essential public services, among other), the government may intercept any kind of communications provided that it is necessary to clarify alleged criminal offenses or to maintain public order (Article 18); and

(c) during the State of Siege, the government directing military and defense policies, shall assume all exceptional prerogatives.

The declaration of a State of Alarm will be conducted by Decree agreed by the Cabinet.

Once the government has obtained an authorisation from the Congress, it shall declare a State of Emergency, by Decree agreed by the Cabinet. The authorisation must include the suspension of article 18.3 of the Spanish Constitution, related to the secrecy of communication, in order for Article 18 LSAES to be applicable.

The government proposes the declaration of State of Siege before the Congress.

Article 122 LJCA refers to the necessary requirements that have to be met in order to obtain judicial authorisation: an initial request by the competent authorities, which has to include the pertinent reasons for the request and also the relevant documents to such purpose. The court, within 24 hours of the request and, after hearing the Public Prosecutor, may issue the requested authorisation, provided that it would not affect Article 18 paragraphs 1 and 3 of the Spanish Constitution.

In accordance with Article 4.5 of the General Communications Act, on the basis of a breach of public service obligations (under Title III General Communications Act), the government, following a mandatory report from the Telecoms Authorities ("**CNMC**"), may exceptionally and temporarily establish the assumption by the General Administration of the direct management of the services or the exploitation of the corresponding networks. Regarding the latter, it may also, under the same conditions, intervene the provisioning of electronic communications services.

4. OVERSIGHT OF THE USE OF POWERS

Pursuant to the Criminal Procedure Act, the relevant court order will determine the extension and scope of the disclosure to be carried out. In this regard, the relevant judge has a duty of supervision to ensure compliance with such court order.

The intervention determined pursuant to Article 18 LSAES shall be notified immediately by reasoned writing to the competent judge.

Countries T-Z

Tanzania

In this report we provide an overview of some of the legal powers under the law of Tanzania that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

The Electronic and Postal Communication Act

The Electronic and Postal Communication Act, 2010 (the "**EPOCA**") does not specifically make provision for interception of customer communications. However, the existence of intercept powers can be implied from section 120 of the EPOCA which provides 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 Tanzania 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 provides that any person who, without lawful authority under the EPOCA or any other written law:

a. intercepts, attempts to intercept, or procures any other person to intercept or attempt to intercept any communications; or

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 having reason to believe that the information was obtained through the interception of any communications in contravention of this section,

commits an offence. 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**") provides 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 TISSA further provides that the Service has the power to investigate any person or body or persons whom or which it has reasonable cause to consider a risk, or source of risk, of a threat to state security and that the Service may conduct any investigations which are required for the purposes of providing security assessments. Section 10 of TISSA provides that the Director-General of the Service shall have the command, control, direction, superintendence and management of the Service and all matters connected with it and that all orders and instructions to the Service shall be issued by the Director-General 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

Pursuant to section 31 of the Prevention of Terrorism Act, 2002 (the "**PTA**"), subject to a police officer obtaining prior written consent from the Attorney-General, he may make an application, ex parte, to the Court for an interception of communications order for the purposes of obtaining evidence of the commission 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 communication service provider;

b. authorising the police officer to enter any premises and to install on such premises, any device for the interception and retention of a specified communication of a specified description and to remove and retain such device,

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.

Criminal Procedure Act

Section 10 of the Criminal Procedure Act [Cap 20 R.E. 2002] (the "**CPA**") provides/grants the powers to police officer(s) to investigate the facts and circumstances of a case where a police officer has reason to suspect the commission of an offence. Further, section 10(2) of the CPA specifically provides for the police officers' powers, by order in writing, to require the attendance of any person (natural or legal) who from information given or in any other way appears to be acquainted with the circumstances of a case, or who is in possession of a document or any other thing relevant to the investigation of a case to attend or to produce such document or any other thing.

2. DISCLOSURE OF COMMUNICATIONS DATA

The Electronic and Postal Communication Act

Section 91 of the EPOCA provides that there shall be a database kept with the TCRA in which all subscriber information will be stored. Every application services licensee must submit to the TCRA a monthly list containing its subscribers information.

Further, Regulation 4(2)(b) of the the Electronic and Postal Communication (Telecommunications Traffic Monitoring System) Regulations 2013 (the "**TTMS Regulations**") provide that the TCRA shall acquire, install, operate and maintain traffic monitoring and measurement devices at the operator's premises. Moreover, regulation 8 of the TTMS Regulations provides, inter alia, that the Traffic Monitoring System shall collect call detail records without any interception of contents of communications such as voice or SMS. Call detail records have been defined as information generated by telephone exchanges which contain details of calls originating from, terminating at or passing through the exchange. In addition, regulation 13(4) of the TTMS Regulations provides that the TCRA must ensure that call detail records data are collected for the exclusive purpose of monitoring compliance with the TTMS Regulations; they are 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 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, pursuant to the Electronic and Postal Communications (Licensing) Regulations, 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 by any permission or approval of the Authority, or as otherwise permitted or required by other applicable laws or Regulations.

Under section 99 of the EPOCA a person shall not disclose any information received or obtained in exercising his powers or performing his duties in terms of the EPOCA except:

(a) where the information is required by any law enforcement agency, court of law or other lawfully constituted tribunal;

(b) notwithstanding the provision of this section, any authorized person who executes a directive or assists with execution thereof and obtains knowledge or information of any communication may;

  (i) disclose such information to another law officer to the extent that such disclosure is necessary for the proper performance of the official duties of the authorised person making or the law enforcement officer receiving the disclosure; or

  (ii) use such information to the extent that such use 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 is reasonable ground for suspecting that an offence under the NSA has been or is about to be committed, and that some person may be able to furnish information with regard thereto, he may, by writing under his hand, authorise a named officer to require that person to give a police officer any information in his power relating to such suspected or anticipated offence.

Tanzania Intelligence and Security Service Act

Section 5 of 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 shall cooperate as far as practicable and necessary with such other organs of state and public authorities within or outside Tanzania as are capable of assisting the Service in the performance of its functions.

Constitution of United Republic of Tanzania

The Constitution of United Republic of Tanzania 1977 as amended from time to time (the "**Constitution**") provides the 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 shall not be void for the reason only that it enables 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, which measures derogate from the right to life.

4. OVERSIGHT OF THE USE OF POWERS

Other than as outlined above there is no judicial oversight over these powers. However, section 114 of the EPOCA provides that the TCRA may take enforcement measures against any person who contravenes licence conditions, regulations and provisions of the EPOCA.

Turkey

In this report we provide an overview of some of the legal powers under the law of Turkey that government agencies have to order Vodafone's assistance when conducting real-time interception and the disclosure of data about Vodafone's customers.

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

The Turkish Constitution

Article 22 of the Turkish Constitution states that interception of communication shall 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, commander of the Turkish gendarmerie forces (at their duty stations) or the director of intelligence agency.

The "law" here can either be a Law, a Decree-Law or a Regulation which is actually below the former within the hierarchy of laws, as per the Turkish legal system. The agency authorised by law includes Information and Communication Technologies Authority ("**BTK**"), establishment of which is required by the Law of Electronic Communications No. 5809 ("5809 sayılı Elektronik Haberleşme Kanunu"). Unfortunately, the term "non-delayable" cases is not a defined term within the Constitution, so it remains open to potentially wide interpretation.

Regulation on Authorisation within the Electronic Communication Sector, published in the Official Gazette no. 27241, entered into force on 27.5.2009 ("Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği") (the "Regulation")

Article 21 of the Regulation empowers the BTK to intercept a communication or suspend, interrupt or stop electronic communication operators from providing a communication 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, BTK shall obtain the opinion of the Transportation and Communication Ministry in order to decide on interception of communications provided by the relevant operator(s).

For the purposes of the Regulation, the word "interception" may also mean suspension, interruption, stopping and/or blocking.

According to the hierarchy of the governmental bodies, BTK is bound to the Ministry of Transportation and Communication; hence the Ministry's opinion shall be taken into account where necessary. 'Where necessary' is an ambiguous expression because there is no absolute ground or application of the occasions that are objectively necessary for the Ministry's opinion.

Regulation on the Procedures Organising the Publications on the Internet, published in the Official Gazette no. 26716 and entered into force on 30.11.2007 ("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 the Presidency of Telecom Communications ("**TIB**") may decide to intercept or block access to the relevant content on the following grounds: "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). The orders of TIB are directly sent to the internet access providers, which includes the operators who provide access to the Internet.

TIB is directly bound to the president of the BTK and serves within the BTK, as per Article 16 of the Regulation for Detecting, Recording and Wire-tapping the Communications, Evaluating the Signal Data, published in the Official Gazette no. 25989 on 10.11.2005 ("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").

As per Article 16 of the Internet Regulation, the order of TIB is sent to the internet access providers, including operators, via electronic means and shall be applied by the access providers within twenty-four hours following the delivery of the order. However; this order shall be subject to legal examination.

The Regulation for the Organisation of BTK, published upon a Decree of Council of Ministers numbered 2011/1688 and dated 4.4.2011, published in the Official Gazette no. 27958 and which came into force on 8.11.2011 ("Bilgi Teknolojileri ve İletişim Kurumu Teşkilat Yönetmeliği" (the "Organisation Regulation")

Article 5/(u) of the Organisation Regulation provides that any and all types of information can be obtained by the BTK from operator enterprises, state institutions, real persons and legal entities, if requested by the Ministry. Therefore operators are obliged to provide the necessary information upon the BTK's request. In Article 5/(ü) of the Organisation Regulation BTK is entitled to take all precautionary actions stated by laws such that activities within the sector are carried out pursuant to the requirements of national security, public order or public services. 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.

Further to this, Article 5/1 of The Regulation on Authorisation within the Electronic Communication Sector published in the Official Gazette no. 27241 and entered into force on 27.5.2009 ("Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği") states that the Transportation Ministry's strategy and policies shall be taken into account while the operators establish the technical infrastructure upon the authorisation given by the BTK. 'Strategy and policies of the Ministry' is another broad term which may conceivably be used by the Ministry to give flexibility to its actions within the communication sector.

Regulation for Detecting, Recording and Wire-tapping the Communications, Evaluating the Signal Data, published in the Official Gazette no. 25989 on 10.11.2005 ("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 higher threshold. The Wire-tapping Regulation gives wiretapping powers to the intelligence bodies, such as the Security General Directorate or Intelligence Head, Gendarmerie General Command etc., 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 spying.

In case 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 for granting security of the government, revealing espionage (spy activities), ascertaining disclosure of state secrets and preventing terrorist activities by the Secretary or/and Deputy Secretary of the National Intelligence Organisation and delivered to the relevant offices for appropriate execution. (Art. 7).

The "relevant offices" mentioned above, where the written orders shall be sent to, appears to be those of TIB. According to Article 10 of the Wire-Tapping Regulation, written orders and decisions shall be sent to TIB via the electronic means determined by TIB. The orders and decisions are then applied under TIB's supervision.

2. DISCLOSURE OF COMMUNICATIONS DATA

Regulation on Protecting the Privacy of Personal Data within Electronic Communication Sector enacted as required by the Law no. 5809 of Electronic Communications, published in the Official Gazette no. 28363

Article 5/(5) of the Regulation on Protecting the Privacy of Personal Data within Electronic Communication Sector, enacted as required by the Law no. 5809 of Electronic Communications, published in the Official Gazette no. 28363 which came into force on 1.1.2014 ("Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunmasi Hakkinda Yönetmelik") (the "**Privacy Regulation**"), provides BTK with the power to access the systems where customer data is collected and stored, if deemed necessary. Because the Privacy Regulation came into force just recently it is not yet clear which occasions are to be treated as "necessary". However, considering this article is located under the sub-heading of "Security", it is assumed this power may be used for security reasons, which may cover public security, preventing crime, prosecuting an alleged crime etc. However BTK is not entitled to access the content of the telecommunication, e.g. listen to the voice content of a telephone call, or read the content of a text message.

The BTK also has power to request all information and documents concerning the security measures taken by operators. It may also request amendments to the security measures taken by the operators if such interference is deemed necessary.

Law no. 5651 on the Regulation of Internet Publications and Prevention of Crime

Under Article 3 (as amended on February 6, 2014) of the Law no. 5651 on the Regulation of Internet Publications and Prevention of Crime, internet access providers must provide communications data requested by the TIB, including a subscriber's name, identity information, address, phone number, date and time of logging into a system, 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, targeted IP address and port number, protocol type, URL address, date and time of connection and date and time of

ending of the connection. These data can only be obtained by TIB where a court order is given in relation to the prosecution of a crime.

The TIB's and the BTK's actions may be brought before the administrative courts for cancellation.

The content of communications cannot be accessed by the BTK or the TIB as per 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

3. NATIONAL SECURITY AND EMERGENCY POWERS

The Turkish Constitution

Intelligence authorities and agencies authorised by law (including the BTK) have the power to intercept communication 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 grounds, as per Article 22 of Turkish Constitution.

According to Turkish Constitution Article 15 and the Law no. 2935 enacted on 25.10.1983 on State of Emergency, communications may be intercepted permanently, or the tools to provide communications to customers may temporarily be seized by reason of public emergency, national security, mobilisation or war.

In case of application of Law no. 2935 enacted on 25.10.1983 on State of Emergency, a declaration of extraordinary administration procedures may derive from a natural disaster or a serious economic crisis, widespread acts of violence and serious deterioration of the public order. The right to communication and the privacy of communication 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.

Also, 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; or in the event of war, the emergence of a situation requiring war, an uprising, or the spread of violent and strong 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, the Council of Ministers, under the chairpersonship of the President of the Republic, after consultation with the National Security Council, may declare martial law in one or 60 more regions throughout the country for a period not exceeding six months.

4. OVERSIGHT OF THE USE OF POWERS

Under Article. 22 of the Turkish Constitution, an authorised agency's order (apart from that of BTK) shall be submitted for a judge's approval in twenty-four hours. The judge's decision shall be declared within forty-eight hours following the submission; otherwise the said order of authorised agency is abolished per se.

The Turkish legal system is based on the continental European legal system. In this respect, the actions/orders/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 take precautionary suspension of administrative actions and then decide on either the cancellation or nullity, or approval of such actions. In that sense, 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 e.g. a Prosecutor's order in an urgent case must be approved by a judge, it appears BTK's actions of interception are not subject to a judge's prior approval. However they can still be subject to litigation before administrative courts for their validity and enforceability.

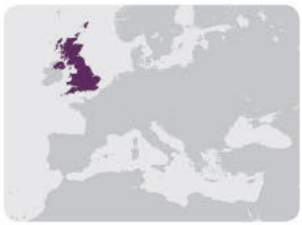
As per Article 17 of the Internet Regulation, if the Prosecutor decides there is no adequate evidence to create suspicion (an 'adequate suspicion' threshold) then the order shall be abolished per se. In urgent cases during the prosecution process, however, the Prosecutors themselves may decide on intercepting/blocking of the content. This decision must be brought before the judge in twenty-four hours and the judge shall decide on the matter within twenty-four 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 order of the Security General Directorate or Intelligence head, Gendarmerie General Command, Secretary of the National Intelligence Organisation, shall be submitted to a judge's approval within twenty-four hours. The judge's decision shall be declared within forty-eight hours following the submission; otherwise the order of the authorised agency is abolished per se.

The decision for conducting the wire-tapping etc. can be given for a period of 3 months at most. This period can be prolonged three times at most for a period not longer than 3 months (i.e. 3x3=9 months).

Intelligence bodies (Security General Directorate, Gendarmerie General Command or National Security Organization) or Prosecutor's decision must be approved by the judge within twenty-four hours following their submission, or the order shall be abolished.

United Kingdom



In this report we provide an overview of some of the legal powers under the law of the United Kingdom that government agencies have to order Vodafone's assistance with conducting real-time interception and the disclosure of data about Vodafone's customers.

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 s.5 RIPA any Secretary of State can issue an intercept warrant where the Secretary of State in question 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 well-being of the United Kingdom and where they believe 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 (s.8 (1) RIPA).

However under s.8 (4) (b) 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 described in such certificate that s/he considers it necessary to examine. RIPA defines the term 'external communication' as a communication sent or received outside the British Islands (s.20 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 Islands, even if they pass outside the British Islands (p.22 of IOC COP).

s.11 (4) RIPA establishes a general requirement on public telecommunication 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 provide assistance in giving effect to a warrant under s.11 (4) the Secretary of State may, under s.12 RIPA, order a public telecommunications service provider to maintain an interception capability. Under s.12 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 provide assistance in relation to intercept warrants. The order is exercisable by the giving of a notice in accordance with such 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 s.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 property so specified or in respect of wireless telegraphy. There is the possibility that this power is broad enough to permit government direct access to Vodafone's network by the Security Services in some instances. Although large parts of ISA have been repealed, s.5 is still in force.

A warrant under s.5 ISA will be granted by the Secretary of State if he is satisfied that the taking of the action by the Security Service, the Intelligence Service or GCHQ is: necessary for the purpose of assisting the particular agency to carry out any of its statutory functions; that the activity is necessary and proportionate to what the agency seeks to achieve and it could not reasonably be achieved by other (less intrusive) means; and that satisfactory arrangements are in place to ensure that the agency shall not obtain or disclose information except insofar as necessary for the proper discharge of one of its functions.

s.11 (1) (a) RIPA provides for the possibility that an intercept warrants can be effected by the LEA or intelligence agency that applied for it without the provision of 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.

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 the metadata relating to customer communications. The powers require anyone who provides a telecommunications service to disclose customer metadata they possess or are capable of obtaining. The powers relate to traffic data, service use information and subscriber information, but not the content of the communications.

Under s.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 s.25 (2) and under the Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010/480).

Under s.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 s.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 for the interests of national security, for the purpose of preventing or detecting crime or preventing disorder, in the interests of the economic well-being of the United Kingdom, in the interests of protecting public safety or for the purpose of protecting 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") the Secretary of State may after consultation with OFCOM and/or providers of public electronic communications networks, give OFCOM or the network provider directions of a general character as appear to the Secretary of State to be necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom. Although the Communications Act 2003 superseded most of the Telecommunications Act 1984, Section 94 is still in force.

Under Section 94, if a network provider is given directions to do or not do something as directed by the Secretary of State they shall not disclose this direction if the Secretary of State has notified them that he is of the opinion that disclosure is against the interests of national security or relations with the government of a country or territory outside the United Kingdom. The Secretary of State may, with the approval of the Treasury, make grants to providers of public electronic communications networks for the purposes of defraying or contributing 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 or public health or in the interests of national security.

Civil Contingencies Act 2004

Under the Civil Contingencies Act 2004 (the "CCA") the government is given broad powers for a limited period of time during civil emergencies. This includes 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 s.1 and s.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 s.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 s.20 and s.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 the purpose of preventing, controlling or mitigating an aspect or effect of the emergency in question.

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 s.57 (1) 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 RIPA s.65, 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 s.12 RIPA notice places unreasonable technical and/or financial demands on it, it may refer the issue to a specialist panel of advisers that is set up under s.13 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 s.12 order and notice procedure is outside the remit of the Interception of Communications Commissioner (s.57 (2) (a) RIPA).

Regarding the disclosure of communications data, under s.37 of the Protection of Freedoms Act 2012 and s.23A and s.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 s.5 ISA. The Intelligence Services Commissioner, appointed under s.59 (1) RIPA, keeps under review the exercise and performance of the powers granted by s.5 ISA. The Commissioner presents an annual report to the Prime Minister, who lays it before the Houses of Parliament and which 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 shall lay before each House of Parliament a copy of every direction given, unless he is of the opinion that disclosure of the direction is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or commercial interests of some other person.

The CCA sets limits on the emergency regulations that can be made under it (CCA. S.23). For example, any emergency regulations must be laid before, and approved by, Parliament as soon as practicable after first being made and in any event they automatically lapse after thirty days (s.26 (1) (a) and s.27 CCA). Emergency regulations may not amend the Human Rights Act 1998 (s.23 (5) (a) CCA). The Houses of Parliament may pass resolutions cancelling the emergency regulations, or amending them (s.27 CCA).