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