# Law Enforcement Disclosure Report

2015

Vodafone Group Plc

# Contents

## Law Enforcement Disclosure Report 2015

**Complex, controversial – and constantly changing** **3**
What we are publishing, and why 4
The transparency challenge 4
Who should publish: governments or operators? 5
What statistics should be reported: warrants or targets? 6
Security and secrecy: the limits on what local licensed operators can disclose 7

**How we work with law enforcement agencies and government authorities** **8**
The Vodafone privacy and law enforcement principles 9
Communications technology and governments 10

**Agency and authority powers: the legal context** **11**
Provision of lawful interception assistance 11
Disclosure of communications-related data 12
Retention of communications data 12
Decryption of protected data 12
Search and seizure powers 12

**Freedom of expression and network censorship** **13**
Telecommunications operators and 'Over-The-Top' internet companies 13
Legal powers to block or restrict access to communications 14
The Vodafone freedom of expression principles 15
How access to communications is blocked or restricted 17
Statistical information 17

**Country-by-country disclosure of law enforcement assistance demands 2015** **19**
Introduction 19
How we prepared this report 19
Explanation of information presented 20
Country pages A-Z 21

## Links

**Previous Report:**
Law Enforcement Disclosure Report 2014

**Legal Annexe:**
Published February 2015

**Legal Annexe:**
Published June 2014

# Law Enforcement Disclosure Report 2015

**This is our second annual transparency report which offers a detailed insight into the legal frameworks, governance principles and operating policies and procedures associated with responding to demands for assistance from law enforcement and intelligence agencies across 28 countries.**

**We have retained much of the explanatory text used in the 2014 report which sets out our principles and practices in what remains a significant area of public debate and concern. However, there are three notable changes to the 2014 report:**

- we have added a new section which focuses on network censorship content blocking and the restriction of services which may impact our customers' ability to express themselves freely. The new section includes a summary of why – and how – governments, authorities and agencies block or restrict access to certain content, services or networks. It also includes a statement of our own beliefs – the Vodafone freedom of expression principles – in addressing what are complex challenges in many countries;
- we have updated our country-by-country summary with the number of lawful intercept and communications data demands received over the preceding year; and
- in February 2015, we updated the legal annexe which summarises the most important legal powers in force in our 28 countries of operation.

During 2014–15, we met a number of stakeholders with specialist interests and expertise in privacy, human rights and freedom of expression issues. We are grateful for their insights and suggestions, many of which we have tried to reflect in this year's report.

## Complex, controversial – and constantly changing

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.

In every country in which we operate, we also 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, content or networks. 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 harm or criminal sanctions, including imprisonment. We therefore have to balance our responsibility to respect our customers' right to privacy and freedom of expression 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.

Communications technologies have evolved rapidly over the last 20 years. More than 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. It is difficult for governments, agencies and authorities to keep pace with such a dynamic and constantly changing industry; in many countries, the legislative framework determining authority and agency lawful access to their citizens' private electronic communications was first defined in an era which predated the consumer internet. 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 environment has proven to be highly controversial. In most countries, governments have incorporated national security exceptions into national legislation to give legal powers to agencies and authorities to access electronic communications. Some governments have constrained those powers to limit their impact on human rights or to apply a human rights test to the use of those powers; others have created much wider-ranging powers with substantially greater human rights impacts. Meanwhile, agencies and authorities can apply advanced analytics techniques – where such activity is lawful – to the information they have required operators to disclose, to the extent that every aspect of an individual's communications, movements, interests and associations can yield 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. This has led to a significant public debate about the transparency, proportionality and legitimacy of the activities of a number of high-profile government agencies and authorities.

Note:

1. Source: ITU



Back to the top

## What we are publishing, and why

This is our second annual law enforcement disclosure report. Few telecommunications operators have joined us in publishing an analysis of law enforcement powers and practices (including information on a country-by-country basis). We welcome the contribution to transparency of those who have; however, as of July 2015 this report remains the most comprehensive of its kind in the world.

The report encompasses all of the 28 local operating businesses under our direct control in which we have received a lawful demand for assistance from a law enforcement agency or government authority between 1 April 2014 and 31 March 2015. 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" franchise relationship) but where Vodafone does not have effective control of a licensed communications operator.

In the 2015 report, we continue to focus on the two categories of law enforcement demands which still 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.

This year's report also includes a new section on the circumstances under which governments, agencies and authorities can order telecommunications operators to:

- block or restrict access to certain websites, content or services; or
- take control of or shut down our network.

We do not include statistical information on the number of demands we receive to block or restrict access to content, services or our networks, for reasons set out later in this report. In February 2015, we updated our legal annexe to include a country-by-country summary of the legal powers which can be used by agencies and authorities to impose the measures summarised above.

This edition of 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;
- disclose the aggregate number of demands we received during 2014–15 in each of our countries of operation unless prohibited from doing so or unless a government or other public body already discloses information on an industry-wide basis (an approach we explain later in this report) and cite the relevant legislation which prevents us from publishing this information in certain countries;
- explain the circumstances under which governments, agencies and authorities can order telecommunications operators to block or restrict access to specific content, services or websites; and
- explain the circumstances under which governments, agencies and authorities can take control of a telecommunications network or order an operator to shut it down.

Compiling this report remains complex and challenging, not least because in certain countries there are potential risks for our employees which arise from our commitment to increase public awareness of the legal powers and operating practices of governments in the area of law enforcement; these can be acutely sensitive matters. As was the case in the 2014 report, we have tried to implement an approach to disclosure that covers 28 countries on a coherent basis. However, in reality there is very little coherence and consistency in law and in 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 in our legal annexe. 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 remains unclear. Wherever possible, we have again approached the relevant authorities to seek clarity. Where it has not been possible to engage with the authorities or where we have been unable to obtain any clarity regarding the legality of disclosure, we have refrained from publishing aggregate statistics on the volume of lawful interception and communications data demands we have received in those countries during 2014–15. It is worth highlighting that in several of the countries where this state of affairs exists, we have been, to date, the only telecommunications operator to explore the potential within the law for a public disclosure of this kind. Where the government has informed us – in response to our enquiries – that we cannot publish statistical information held for our own operations in the country in question, we have complied with that instruction; to have done otherwise would put our employees at risk of some form of sanction or potential harm and would risk the revocation of our licence to operate, preventing us from providing services to our customers.

In a number of countries, we sought to engage with the authorities throughout 2014–15 to discuss options for enhanced transparency through the publication – by government – of aggregate, industry-wide statistical information. We summarise our actions in the country-by-country section of this report and will continue to pursue further discussions over the year ahead.

## 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.

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 or 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 that a single demand has been issued 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.

In a number of the countries in which we operate, other operators have begun to publish statistical information related to some of the law enforcement demands received for their own operations. In our view, however, inconsistent publication of statistical information by individual operators amounts to an inadequate and unsustainable foundation for true transparency and public insight. It is certainly no substitute for comprehensive disclosure by government with – ideally – independent oversight. 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 the only genuinely meaningful statistic would be the number of individual people who had been targeted by agency and authority demands over a given period, typically one year. However, for the reasons explained below, that statistic is not visible even to an individual operator with respect to their own customers, let alone across the industry as a whole. Although regulators, parliaments or governments will always have a far more accurate view of the activities of agencies and authorities than any one operator, given the number of different authorities involved and the need for confidentiality between them, even a national regulatory body is unlikely to be able to collate comprehensive information by target.

We have therefore concluded that the most pertinent available statistic is the number of warrants issued. However, our belief is not without qualification. In order for the 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, ideally by an independent regulatory or parliamentary body;
- 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 all 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 continue to discuss the opportunity for the authorities – in a number of different countries – to enhance the level of transparency provided through government disclosure in the 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 for 2014–15. However, our concerns about the inadequacy of this kind of disclosure remain. Wherever possible, we have tried to work with other local operators to discuss the best way to develop a consistent cross-industry recording and reporting methodology and have engaged with a number of governments, agencies and authorities to make the case for a central, independent and verified source of statistical information spanning all operators.

Finally, we would emphasise that it is still 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 recorded and reported (where public disclosure 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 mean that attempts to analyse year-on-year movements within any particular country are of questionable value. An apparent sharp increase or decrease in demand volumes from one year to the next may indicate a shift in the scale or pace of law enforcement activity; however, equally it may arise as a consequence of changes in reporting methodology.

**What statistics should be reported: warrants or targets?**

In our country-by-country disclosures, we have focused on the number of warrants (or broadly equivalent legal mechanism) issued to our local operating 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 28 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. It is worth noting that in the majority of countries we report on, 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, not to mention those with whom the individuals targeted may have communicated. The scope for miscounting is therefore immense.

In our view, given the inherent difficulty of drawing reliable conclusions from statistics related to target numbers, 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.

**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 or our business. 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 national 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 or revocation of our operating licence.

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. While we can – and do – challenge demands that are not compliant with legal due process or seem disproportionate, it is however 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 may be unlawful, could lead to some form of sanction against our local business and – in some countries – would also present an unacceptable level of risk of harm for individual employees, to whom Vodafone owes a duty of care, both in law and from a human perspective as a responsible employer.

While 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 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 on 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 Vodafone Group 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 agencies and 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 legal due process.

Demands for assistance made by agencies or authorities acting beyond their jurisdiction will always be refused, in line with our principles; the agency or authority in question would be told to pursue a government-to-government Mutual Legal Assistance Treaty (MLAT) procedure 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 following three categories.

### *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 while 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 agencies and authorities on a voluntary basis to seek to prevent or investigate criminal or malicious attacks – including 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. 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.

## The Vodafone privacy and law enforcement principles

Please note that our privacy and law enforcement principles are largely consistent with those set out in the 2014 report with one change only to highlight the potential for specific exceptions where there is a significant risk to safety of life or the safety of our employees.

**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 legal due process when responding to demands for access to customer data, other than in specific safety of life emergencies (such as assisting the police with an active kidnapping event) or where refusal to comply would put our employees at risk; 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 law enforcement assistance 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 as laws and technologies evolve), we have three objectives:

### *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 European Union. 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 help us to manage that tension in a manner which protects our customers and reduces the risks to our employees without compromising our principles.

**Communications technology and governments**

It is inevitable that legislation lags behind technological innovation in the fast-moving and complex era of IP-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, however, that 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 updates of the aggregate number of agency and authority 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. While 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 a citizen's right to 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 telecommunications 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 legal annexe 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 legal annexe, an updated version of which was published in February 2015.

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 real-time interception of the content 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 at the point at which they 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 will 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 here.

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.

## 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 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 access to communications data as the relevant agencies and authorities already have permanent access to customer communications via their own direct link.

Vodafone's networks are designed and configured to ensure that agencies and authorities can only demand access to data held within the country in question, and our local subsidiaries will only disclose data to an appropriately authorised agency or authority operating under a legal mandate within that country's jurisdiction. So, for example, an Italian agency can only demand access to data held within Vodafone Italy's operations or transmitted across Vodafone Italy's networks.

If an agency or authority wishes to demand access to communications data held abroad on another Vodafone network, they must initiate a Mutual Legal Assistance Treaty (MLAT, also known in Europe as a European Investigatory Order) request – on a demand-by-demand basis. A MLAT enables agencies and authorities in different countries to coordinate and share information through a process overseen by the respective governments involved, although it is important to note that operators typically cannot see if a particular demand originates from within a national agency or authority or has been initiated in response to a MLAT request from an agency or authority in another country. MLAT arrangements can only be used to obtain evidence for criminal investigations and prosecutions.

## 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 section of our Group 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. What data must be retained – and for how long – is a matter of public debate in a number of countries as governments pursue legislative changes to redefine the duration and scope of data retention requirements. 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 prepaid mobile phone services where no identity information is otherwise needed to bill for the service.

## Decryption of protected data

Communications services are increasingly encrypted in some form to restrict unauthorised access. This encryption 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 keys 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. Over time, it is likely that there will be increasing tension between individual governments and the providers of encrypted services whose operations are based in a foreign jurisdiction and therefore beyond domestic legislative reach.

## 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.

# Freedom of expression and network censorship

Our business is focused on connecting people and helping them manage every aspect of their digital lives. Ensuring our customers are able to use our networks and services confidently and free of unreasonable constraints is integral to our commercial success.

Freedom of expression is enshrined in international law and enacted through national legislation. Measures which allow citizens to increase their knowledge and understanding and encourage greater institutional openness and transparency are central to the wider promotion and protection of human rights.

We are a significant investor in many of the countries in which we operate. Widespread prosperity is critical to the achievement of returns on those investments; the greater our customers' participation in their country's economy, the more likely they are to use our services. Social cohesion and inclusion – which are linked, in part, to freedom of expression considerations – are important factors in determining the extent to which a community or nation will experience enduring prosperity and growth. For that reason, we include a comprehensive assessment of those factors in our decision-making processes when considering whether or not to invest in a new country for the first time.

All governments reserve the right to limit their citizens' ability to access and use digital networks, services and content under certain circumstances. This new section of the report provides an overview of the challenges faced by telecommunications operators in seeking to respect their customers' right to freedom of expression. We summarise here the circumstances under which governments, agencies and authorities can order telecommunications operators to:

- shut down or take control of all or parts of a network;
- block or restrict access to specific communications services; and
- block or restrict access to specific websites or content.

In February 2015, we updated the legal annexe to this report to provide, on a country-by-country basis, an overview of the categories of legal powers used by governments, agencies and authorities to achieve the outcomes above.

We have also set out below our own statement of principles in relation to matters of freedom of expression, together with our beliefs regarding what, in our view, governments should and should not do in this area.

**Telecommunications operators and 'Over-The-Top' (OTT) internet companies**

Our core business is connectivity. We operate physical network infrastructure assets (such as mobile phone towers, fibre-optic cables and data centres) which our customers use to communicate and to access content. Our focus is on ensuring that the vast volumes of data which pass through our networks every day reach their intended destination as quickly, efficiently and securely as possible.

While telecommunications operators can be ordered to block access to certain content (as we explain earlier in this report), in practice they serve as the conduit used by customers to access content, not as the creators or commissioners of the material in question. Operators therefore do not have direct editorial control over the very large majority of content and services which flow through their networks.

Unlike Vodafone, 'Over-The-Top' (OTT) internet companies such as Facebook, Twitter and Google do not operate their own communications network infrastructure (beyond some relatively limited projects). The OTT companies' core business is providing content and communications services to their users; they have a much greater degree of editorial control over both the services and apps they make available to their users as well as over the content (videos, photos and text) hosted on their servers, an increasing proportion of which is user-generated.

OTT companies can choose which content they wish to upload, promote or remove and have established teams and systems to enforce their 'house rules' on acceptable content. To provide a practical example: if an individual accesses a Facebook page using a smartphone connected to a Vodafone network and wishes to complain about the content, only Facebook can respond to that complaint, assess the content in question and, if appropriate, remove it; Vodafone cannot alter or take down (or, if only shared privately, even read or view) the content. As a result, OTT companies receive far more complaints and takedown demands (from their users as well as from authorities and agencies or the courts) than any telecommunications operator.

Over time, drawing a clear distinction between telecommunications operators and OTT companies will become increasingly difficult. As the telecommunications market converges with the TV market and more customers buy quad-play packages (a single contract which includes mobile, TV, fixed-line broadband and calls), telecommunications operators will increasingly host commercial content (such as movies and TV shows) on their own servers. It is also conceivable that operators may begin to host large volumes of user-generated content at some point in the future. Those developments would mean that operators would be in a position to exert a degree of direct editorial control over the material provided to their customers and would therefore need to develop the kind of content policies and procedures followed by OTT companies and others.

## Legal powers to block or restrict access to communications

Governments retain the legal power to block or restrict access to communications for a variety of reasons. Their need to do this can be justified under limited circumstances, which we consider below.

There are other ways in which a telecommunications operator can be compelled to prevent its customers from accessing specific services and content. For example, a court can issue an order related to the infringement of intellectual property rights or defamatory material. Operators also block access to certain content – such as spam and malware – in their own right for the reasons we set out in our freedom of expression principles, below.

However, it is the extent to which the state (via its agencies and authorities) can determine what their citizens can see, read or share online – or whether or not they can communicate at all – which is the primary focus of this section of our report as this, in our view, is the area of greatest public concern and debate.

There is a range of powers and measures available to governments to block or restrict access to communications services, the most salient of which are listed below.

### *National security powers*

The protection of national security is a priority for all governments. This is reflected in the legislative frameworks created by governments which grant additional powers (under national security powers) to agencies and authorities engaged in national security matters which typically exceed the powers available for domestic law enforcement activities. For example, in many countries, domestic law enforcement legislation seeks to achieve a balance between the individual's right to privacy and society's need to prevent and investigate crime; however, 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.

### *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 require telecommunications operators to prevent access to certain content or websites identified by their internet protocol (IP) address ranges or uniform resource locators (URLs). This is typically achieved by means of requiring a filter to be applied at the network level.

Hosting illegal child abuse content is considered to be anathema in many countries and as such is widely blocked, either under a court order, a standing legislative requirement or on a voluntary basis under the Internet Watch Foundation or an equivalent scheme. Other forms of online content may also be filtered according to a 'block list' maintained by the relevant agencies or authorities which is then imposed upon operators and service providers under legal due process.

### *Takedown of services*

Many countries empower agencies and authorities to order operators to take down specific communications services, typically in order to restrict access to information which the government considers harmful to social order. Agencies and authorities may also be empowered to order operators to impede the ability of certain groups to coordinate their activities via digital communications. Messaging services and social networks are familiar targets for these takedown actions; however, actions of this nature rarely prove effective over the longer term given the dynamic adaptability of some internet applications and protocols.

### *Emergency or crisis powers*

All countries have some form of special legal powers that can be invoked at a time of national crisis or emergency such as during a major natural disaster or the outbreak of violent civil unrest. The scope and use of those powers is typically overseen by 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.

While 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 forced all operators – including Vodafone – to shut down their networks entirely. An overview of those events (and Vodafone's response to them) can be found here. Further details of the legal powers available to agencies and authorities in each of our countries of operation are set out in our legal annexe which was updated with additional content in February 2015.

On a much smaller scale, a number of countries also retain legal powers to require telecommunications operators to ensure enough bandwidth is available to designated SIM cards in mobile phones used by the emergency services at the scene of a major incident if networks become congested within the immediate local area. In reality these powers are rarely used and are wholly ineffective unless the emergency services have ensured in advance that telecommunications operators have an up-to-date list of the SIM cards to be prioritised.

## The Vodafone freedom of expression principles

In practice there are very few global absolutes in freedom of expression. Societal norms, cultural taboos, religious and national sensitivities have all shaped local laws that are designed to place boundaries around the citizen's right to express themselves freely.

This is a complex area which raises numerous questions that can be challenging to answer. For example, at what point does satire become offensive? What tips the risqué over into the obscene? What separates feisty political challenge from constitutional contempt? Why are some interpretations of history criminalised but others celebrated? Why is an image considered to be art in one country but illegal pornography in another?

As our legal annexe shows, the circumstances under which agencies and authorities can use their legal powers to require us to block or restrict access to our network or to online services and content vary greatly from country to country. Defining a set of robust and meaningful principles that can feasibly be put into practice across all of Vodafone's operating companies worldwide is, therefore, a significant challenge. There are wide disparities in legislation between countries and cultures and even between neighbouring member states within the European Union which are closely aligned in many other ways.

Certain local laws (and the actual practices of agencies and authorities empowered under those laws) will be in conflict with our principles. However, we are compelled under the terms of our licences to comply with national legislation and, as we explain earlier in this report, our employees face the risk of criminal sanction – including potential imprisonment – if they refuse to obey a lawful instruction. Protecting their liberty and safety is one of our highest priorities. Non-compliance could also lead to the loss of Vodafone's operating licence in that country.

Our freedom of expression principles expand on our business principles (which are contained within our Code of Conduct) and have also been informed by international laws, standards and reports, including:

- the Universal Declaration of Human Rights;
- the International Covenant on Civil and Political Rights;
- the International Covenant on Economic, Social and Cultural Rights;
- the UN Guiding Principles on Business and Human Rights;
- the UN's 'Protect, Respect and Remedy' Framework;
- the OECD Guidelines for Multinational Enterprises; and
- the reports of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.

**We do:**

- respect and seek to protect our customer's lawful rights to hold and express opinions and share information and ideas without interference;
- seek to challenge agency or authority demands that appear to us to be overly broad, insufficiently targeted or disproportionate in nature;
- honour internationally recognised human rights laws to the fullest extent possible while also meeting our obligations to comply with local laws;
- seek to increase public understanding – within the limits of lawful disclosure – of the powers and practices used by agencies and authorities in pursuit of mandates which may restrict freedom of expression;
- seek to persuade governments, agencies and authorities – where feasible – to implement measures that minimise or mitigate the impact on freedom of expression arising from the implementation of a lawful demand;
- seek to influence and inform the development of laws relevant to our industry – where we have the opportunity to do so – in order to limit constraints on freedom of expression to narrowly defined circumstances based on internationally recognised laws or standards[2]; and
- seek to intervene at the highest possible levels should our employees come under duress as a consequence of their refusal to process an agency or authority demand that is unlawful.

**We do not:**

- go beyond what is required under legal due process when responding to demands other than where refusal to comply would put our employees at risk; or
- block access to services or content beyond measures that are:
  - specified in a lawful demand from an agency or authority;
  - undertaken under the IWF or equivalent schemes that are designed to prevent access to illegal online child abuse material;
  - defined and implemented by the customer directly through parental controls software or other user-defined filters, with simple and transparent opt-in and opt-out mechanisms; or
  - undertaken to protect the integrity of our customers' data, manage traffic or prevent network degradation, for example blocking spam or malware or taking action to prevent denial of service hacker attacks.

**We believe governments should:**

- establish legal frameworks governing freedom of expression which are clear, unambiguous and publicly explained;
- ensure national laws that interfere with freedom of expression are limited to the necessary not the possible, restricting intervention to those measures which are proportionate, carefully targeted and consistent with internationally recognised human rights laws and standards;
- ensure, under those frameworks, that each individual agency or authority action restricting freedom of expression requires prior authorisation by a publicly accountable senior figure (such as a minister or a judge) who would be responsible for verifying that the authorisation sought conformed to the legally defined purpose;
- establish an entity to provide independent oversight, providing it with legal powers to compel all parties (including agencies, authorities and companies) to supply all information required to assess compliance with due process;
- commit to full transparency in disclosing to a parliamentary committee, constitutional court or similar publicly accountable body, the extent to which agencies and authorities had complied with due process over a given period;
- publish – at least annually – relevant and meaningful statistical information related to the number of agency and authority demands issued to block or restrict access to services or content; and
- ensure their citizens are made aware whenever access to specific content has been blocked for legal reasons, for example by permitting telecommunications operators and service providers to supply an online 'splash page' instead of a simple '404 page not found' error message.

Note:

2. The narrowly defined circumstances should be taken from Article 19 of the International Covenant on Civil and Political Rights (ICCPR); specifically, the actions necessary to:
   - preserve national security and public order;
   - protect public health or morals; or
   - safeguard the rights or reputations of others.

   The scope of permissible restrictions provided in Article 19(3) of the ICCPR is read within the context of further interpretations issued by international human rights bodies, including the Human Rights Committee and the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. The UN Special Rapporteur has identified exceptions to freedom of expression that states are required to prohibit under international law, specifically:
   - child sexual abuse imagery;
   - direct and public incitement to commit genocide;
   - advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence; and
   - incitement to terrorism.


Back to the top

## How access to communications is blocked or restricted

There are a range of different methodologies that telecommunications operators can use when required to respond to an agency or authority demand for a block or restrictions on networks, services or content.

When a telecommunications operator is served with an order to shut down communications in a specific region or across its entire national network, the priority of the managers within the network operations centre (NOC) is to ensure that the enforced shutdown is carefully controlled to enable the network to be restored as quickly and reliably as possible once the government order is lifted. This includes disabling any automated procedures that are designed to mitigate the impact of unexpected network outages.

The shutdown of a specific region within a national mobile network is more straightforward than attempting to shut down communications across landlines in a defined area, as managers in the NOC can remotely deactivate the radio transmission infrastructure (base stations and masts) in a specific location. It is also relatively straightforward to shut down – and, later, restore – voice and text services; however, mobile data services are more complex.

Telecommunications operators have a number of technical options available to block access to specific online content, all of which are based on checking the customer's request to access a specific IP address or URL against a list of banned domains or URLs.

Governments generally stipulate the minimum technical specifications of the restrictions to be applied to the network, content or services in order for operators to fulfil demands received from agencies and authorities. Some technical options are more robust than others; web-proxy content filters hosted within an operator's network are the most expensive but also the most effective approach. In the majority of cases, web traffic passes through the operator's proxy servers. If the content the customer wishes to access is not on the block list, the content sought will be retrieved and served back to the customer. If it is on the block list, best practice is to ensure the customer is made aware of this by means of a warning 'splash page' while preventing the specific content from being accessed; a point we address above.

Domain/URL block lists are typically supplied to operators as a regularly updated dynamic database which is downloaded from an external source then uploaded onto the proxy servers within the operator's network. List entries may refer to a single IP address or they may refer to an entire website domain or sub-domain. A court order focused on a specific website would generally require a manual intervention to block the specific URL on the operators' proxy servers.

Although experienced computer users (and hackers) can bypass most web-proxy filters, these technical measures are effective in preventing many people from gaining access to content deemed to be unlawful by agencies and authorities. However, if the internet connection is fully encrypted end-to-end and the telecommunications operator does not have the key to decrypt the data, it may not be possible for the operator to identify the source or destination of the traffic passing through its network which in turn compromises the effectiveness of the network filters. As services with built-in end-to-end encryption proliferate, it is likely that governments, agencies and authorities will become increasingly concerned if blocking and filtering technologies become less effective as a consequence.

## Statistical information

In our report last year, we said we would explore the feasibility of including statistical data regarding agency and authority demands to block or restrict access to services and content. Since then, we have worked with our colleagues across 28 countries to gain an understanding of:

- what statistical information we capture and hold in each of our local markets;
- how other telecommunications operators and service providers seek to address the need for freedom of expression statistical information;
- the legal limitations on disclosure on a country-by-country basis and consequent potential risks to our employees arising from publication of data in an area which – for some governments – is highly contentious and sensitive; and
- the extent to which a statistical approach could help inform public understanding of the issues in question.

As a result of this research we have concluded that unfortunately, at present, it is not possible for Vodafone to present a meaningful statistical analysis of government efforts to block or restrict access to services or content. Furthermore, we believe that some of the statistical approaches used to date act, if anything, as a barrier to transparency as the methodologies used are hugely variable and disjointed.

To provide a theoretical illustrative example, if a government ordered all operators to block access to a social media network for a period of two weeks, that action could be recorded as:

- one action (the government's single order);
- 14 actions (on the assumption that the block list was updated daily);
- around 400 actions (if the block list was updated dynamically every hour; quite likely if the government continually sought to block attempts to re-route to alternative IP addresses); or
- around 4 million actions (the estimated number of in-country unique users of the social network affected, although some would take advantage of dynamic re-routing to bypass the state-imposed filters, as explained above).

While it could be argued that the largest metric is the most meaningful, would a government that mandated the blocking of any blog or social media posting containing a particular keyword of interest to a small number of campaigners pursuing a niche single issue be less of a threat to freedom of expression than a government whose only intervention in one year was to require the blocking of a single video on a service accessed by 100 million people?

To make matters more complex, a single blocking order could list multiple domains or URLs, or multiple blocking orders could relate to a single domain or URL. Compounding the challenge further, different governments, parliaments, regulators, agencies and authorities apply a wide variety of definitions when authorising or recording the types of demands outlined in this report.

In addition, there are variations in counting methodologies between different telecommunications operators and 'Over the Top' (OTT) internet companies (such as Facebook or Google) as each is subject to different legal and regulatory regimes. Finally, Vodafone's subsidiaries also operate under a variety of licence conditions and local legal requirements, with a consequent wide range of counting methodologies: it is therefore difficult to achieve consistency even within our own company.

In our view, the obligations for governments that we set out in our freedom of expression principles to publish this information at least annually, would provide, in aggregate, the most significant enhancement to transparency in this area and would help address many of the concerns expressed by campaigners and individual citizens about an important and often highly controversial aspect of state intervention in digital communications.

Further details about the situation in each of our countries of operation are set out in our country-by-country disclosure of law enforcement assistance demands section overleaf, together with statistical information about the number of demands received where it is legal to publish them and authorities do not already do so.

# Country-by-country disclosure of law enforcement assistance demands 2015

**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. Note that Vodafone no longer operates in Fiji; this country is therefore no longer included in this section of the report.

As we explain earlier in this report, this remains a difficult section to compile. There is still no established model to follow: few international telecommunications 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 telecommunications 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.

Over the last year, we have sought to engage with a number of governments, agencies and operators to explore options for a more consistent and meaningful approach to statistical recording and public disclosure which would enable a greater level of overall transparency. While there was some progress in some areas, on the whole it has proven to be very difficult to persuade others of the case for changes which would bring a higher level of coherence to any statistical analysis of the data presented in this report. Updates on our efforts to enhance transparency in individual countries can be found in the relevant country reports.

## 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 will not typically be made aware of the context of any demand.

Although the details of individual demands remain highly confidential and cannot be communicated, Vodafone's internal auditors conduct regular reviews of the overarching processes and policies that are in place to ensure the integrity of our law enforcement disclosure systems. However, it is not possible for the external assurers of the Vodafone Group Sustainability report, EY, to provide any form of independent verification of the statistical information published in this section for the reasons stated above.

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, while 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.

Our global internal review which analysed, 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, remains relevant with no changes to note.

As was the case in the 2014 report, we have also published a legal annexe. In compiling this annexe, we instructed the law firm Hogan Lovells to provide us with objective and independent advice which was then verified by our legal teams in each of our operating country businesses[1]. The legal annexe was updated and republished in February 2015 to include new information focused on network blocking and censorship, including the:

- shut down of network or communication services;
- blocking of access to URLs and domains; and
- powers enabling agencies and authorities to take control of a telecommunications network.

As we noted in our 2014 report, it remains the case that in some countries there is a lack of legal clarity regarding disclosure of the aggregate number of law enforcement demands. Where this continued to be the case in 2015, we have, once again, sought to engage with governments to ask for guidance wherever this was practicable in light of the potential risks to our employees.

Notes:

1. Vodafone is 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.

In a small number of countries where the government does publish statistics but where there remain concerns regarding the methodology used in recording and/or reporting this information, we summarise the discussions undertaken to try to enhance transparency in the relevant country section. Further information about our approach under those circumstances is set out earlier in this report.

Some governments responded to our requests for guidance: their views are summarised in the relevant country section in this section of the report. Others continued to decline to reply to our enquiries altogether or have made it known to us that they remain reluctant to provide any indication of their perspectives. Where this is the case, we have taken a precautionary approach to protect our employees.

Finally, in countries experiencing continuing periods of significant political tension, it remains challenging to ask any questions related to national security and criminal investigation matters – however seemingly innocuous – without potentially putting Vodafone employees at risk of harassment or criminal sanction.

## 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, we have noted our concerns about the considerable shortcomings inherent to this approach, as explained earlier in this report.

One year on from our first report, it is even clearer to us than was the case in 2014 that in those countries where the government publishes certain statistical information and individual operators also publish some of the statistics held for their own operations, the net effect is more confusing – and in statistical terms, irreconcilable and contradictory than if the governments involved played a greater role in enabling the provision of consistent and comprehensive metrics spanning the industry as a whole.

In countries where these statistical anomalies arise, we will continue to engage with other operators, industry, authorities, and at a ministerial level to press for greater consistency and enhanced transparency in governmental disclosures. We will continue our efforts in this regard and will update the country sections of this report in future if there are any relevant developments.

It is also important to emphasise that attempts to compare one country's metrics with those of another are essentially meaningless given the very wide variations between legal frameworks, recording methodologies and reporting regimes. There are no consistent points of common reference that could be used to underpin such analysis. Similarly, in many cases it is difficult to draw accurate conclusions from year-on-year changes in reported metrics within a country as these can be influenced by a range of factors – such as amendments to legislation or new laws, developments in agency or authority practice or changes to the approach used to log, aggregate and disclose lawful demands – which may not in themselves provide a reliable indication of actual trends in law enforcement activity.

There are five 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 legal 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. 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.

**4. Cannot disclose**
Although local laws do not expressly prohibit disclosure, the authorities have told us directly that we cannot disclose this information.

**5. Government/other public body publishes**
In a number of countries, the government, parliament or a credible independent public 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.

# 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. Links are provided to the individual government reports that are referenced in many of the country tables below. A summary of the most important legal powers relating to law enforcement demands and network censorship, on a country-by-country basis, can be found in the legal annexe, last published in February 2015.

| Albania | | |
|---|---|---|
| | Type of demand | |
| | Lawful Interception | Communications Data |
| Statistics | Vodafone disclosure unlawful (1) | 5,695 (2) |
| Key note (1) | It is unlawful to disclose any aspect of how lawful interception is conducted. | |
| Key note (2) | Prior to the 2014 report, the legal position was 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 were informed that we could disclose this information in the 2014 report. There has been no change to the guidance since that report: we have therefore updated this statistic with the latest information we hold for our own local operating business. | |

| Australia | | |
|---|---|---|
| | Type of demand | |
| | Lawful Interception | Communications Data |
| Statistics | Government/other public body publishes (1)<br>Further action to follow (2) | Government/other public body publishes (1)<br>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) | The Australian government has legislated for a communications data storage regime to be implemented from October 2015. Telecommunications operators will be required to retain the proscribed information for two years. The period of time stipulated for the storage of communications data is at the upper bounds of the requirements implemented or proposed in other jurisdictions. However, the legislation establishes a range of assurance measures – including oversight by the Commonwealth Ombudsman – and there will be a reduction in the number of agencies permitted to issue demands for access to that information.<br><br>During the consultation phase of the communications data storage legislative process, we engaged with the Attorney General and made submissions to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) regarding the reporting regime for the recording and disclosure of statistics related to law enforcement demands.<br><br>The Australian government has now accepted the PJCIS recommendation that the Telecommunications (Interception and Access) Amendment (Data Retention) Act should require the Attorney General to provide a public report on an annual basis stating the number of law enforcement demands for access to communications data together with the age of the data sought.<br><br>We believe this would represent an important enhancement to transparency and welcome the government's decision to adopt the PJCIS recommendation. Discussions regarding further refinements to the reporting regime – including a common approach to industry disclosure – are ongoing. We are urging the government to finalise those arrangements as part of the implementation of new legislation regarding the storage of communications data.<br><br>Meanwhile, another operator in Australia has published information related to some of the statistical data it holds for its own operations. As we explain earlier in the report, while transparency is important, we do not believe that individual operator disclosures of this kind are an effective route to achieve the level of transparency sought by the public as a whole. We will therefore continue to engage with government and industry to ensure that the new policy framework contains statistical data reporting provisions which are as consistent and robust as possible. | |

| Belgium | | |
|---|---|---|
| | Type of demand | |
| | Lawful Interception | Communications Data |
| Statistics | No technical implementation (1) | 0 |
| 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 | 8,583 | Government/other public body 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) | 506 |
| 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. | |

| Egypt | | |
|---|---|---|
| | Type of demand | |
| | Lawful Interception | Communications Data |
| Statistics | Vodafone disclosure unlawful (1) | Vodafone disclosure unlawful (1) |
| Key note (1) | While the precise legal position regarding disclosure of aggregate statistical information remains 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. | |

| 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/other public body publishes (1)<br>Further action to follow (2) | Government/other public body publishes (1)<br>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.<br><br>The German Federal Office of Justice publishes annual statistics related to agency and authority demands for access to communications data.<br><br>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) | During the process to compile the 2014 report, it became apparent that the legal position regarding the disclosure of lawful interception and communications data demands was unclear. The following were relevant in our assessment of the legal position:<br><br>• 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; and<br>• 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.<br><br>Prior to the publication of the 2014 report, it was therefore unclear whether or not we could lawfully publish the statistical information we held for our own operations. Furthermore, prior to the 2014 report we were instructed by the Federal Network Agency (BNetzA) that publication of the information we held for our own operations in Germany was prohibited.<br><br>Subsequent to our discussions with the BNetzA and following the publication of statistical information held by another operator, the Federal Ministry of Justice (BMJV) clarified that publication of statistical information by individual operators is lawful.<br><br>However, disclosures presented by an individual operator offer – at most – only a partial view of law enforcement demands (for example, they excluded the effect of German agency and authority automated access systems which allow rapid and large-scale interrogation of a central database of customer records) and could not be reconciled with the authorities' publication of the number of warrants issued each year.<br><br>In addition, the statistical information published by another operator was based on the number of targeted subscribers rather than warrants received. It is impossible to reconcile those metrics with the methodology used in the government's own disclosure regime, raising an even greater risk of miscounting than arises when an individual operator publishes statistical information derived from the number of warrants it has received.<br><br>While Vodafone Germany's demand volumes when measured on a targeted subscriber basis are broadly in line with those of the other operator to report using this methodology, the fundamental misalignment between the two statistical reporting approaches – warrants versus targeted subscribers – makes it impossible to draw any reliable conclusions from the data available.<br><br>During 2014–15, we wrote to the authorities and members of parliament to raise a number of issues and concerns around privacy and law enforcement activities. Over the coming year, we will seek further engagement with the government and other operators to press the case for the development of a more coherent and robust disclosure framework. | |

| Ghana | | |
|---|---|---|
| | 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 remains unclear regarding whether or not it would be lawful for Vodafone to disclose statistics related to agency and authority communications data demands.<br><br>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.<br><br>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.<br><br>Prior to the publication of the 2014 report, we approached the authorities to ask for clarity and guidance as to whether Vodafone was lawfully permitted to disclose aggregate statistics related to communications data demands received from government agencies and authorities. We did not receive a response in time for publication of last year's report.<br><br>During 2014–15, we have again attempted to engage with the authorities to seek guidance but have again been unable to obtain clarity on the legal position. Given the uncertain legal position and the extent of potential risk to our employees associated with publication, we are therefore not in a position to disclose aggregate statistics related to communication data demands. | |

| Greece | | |
|---|---|---|
| | Type of demand | |
| | Lawful Interception | Communications Data |
| Statistics | Government/other public body publishes (1) | Government/other public body 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) | 76,530 (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.<br><br>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.<br><br>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.<br><br>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 Licence (UASL: the licence governing access service in India), and Clause 33.5 of the Internet Service Provider (ISP) Licence (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 comes under the purview of these provisions. | |

| Ireland | | |
|---|---|---|
| | Type of demand | |
| | Lawful Interception | Communications Data |
| Statistics | Cannot disclose (1) | 7,973 |
| Key note (1) | Prior to publication of the 2014 report, we approached the authorities to seek clarity on the disclosure of aggregate statistics related to lawful interception demands. In response, the authorities instructed us not to disclose this information.<br><br>During 2014–15, we engaged extensively with the government to discuss whether or not such information could be published by the authorities themselves or – if not – by Vodafone and other operators. The government has again informed us that we cannot disclose this information. | |

| Italy | | |
|---|---|---|
| | Type of demand | |
| | Lawful Interception | Communications Data |
| Statistics | Government/other public body publishes (1) | 866,578 |
| Key note (1) | While the latest report currently available on the Ministry of Justice website does not include the 2014 lawful interception statistics, we have a reasonable expectation that the Ministry intends to update these statistics in due course. | |

| 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 remains 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.<br><br>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.<br><br>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.<br><br>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.<br><br>Under the current circumstances, we have concluded that it is still not 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) | 595 |
| 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) | 3,339 (2) |
| Key note (1) | It is unlawful to disclose any aspect of how lawful interception is conducted. | |
| Key note (2) | Prior to the 2014 report, the legal position was 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 were informed that we could disclose this information in the 2014 report. There has been no change to the guidance since that report: we have therefore updated this statistic with the latest information we hold for our own local operating business. | |

| 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 remains unclear regarding whether or not it would be lawful for Vodafone to disclose statistics related to agency and authority communications data demands.<br><br>Over the course of the coming year, we will attempt to engage with the new government, agencies and authorities 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)<br>Government/other public body publishes (2)<br>Further action to follow (3) | Government/other public body publishes (2)<br>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) | Prior to publication of the 2014 report, we approached the Ministry of Security and Justice to urge the government to take action to address the wide variations in methodology used by operators, governments and others in recording and reporting statistical information which we believe have the effect of acting as a serious barrier to meaningful public transparency.<br><br>In response, the Ministry committed to form a cross-functional working group – including Dutch operators – to consider options to increase the quality of public transparency. Unfortunately, there was little progress during 2014–15 on the need for change to the current reporting methodology.<br><br>As we explain earlier in this report, we believe that governments – not operators – should take responsibility for the publication of aggregated statistical information related to agency and authority demands. We have therefore approached the new Minister and the new State Secretary of Security and Justice to discuss these issues once again, and over the coming year we will continue to engage with the government in an effort to improve the quality of transparency via the creation of a more coherent and robust disclosure framework. | |

| New Zealand | | |
|---|---|---|
| | Type of demand | |
| | Lawful Interception | Communications Data |
| Statistics | Government/other public body publishes (1) | Government/other public body 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:<br>• The New Zealand Police<br>• The New Zealand Security Intelligence Service<br>• The New Zealand Serious Fraud Office<br>• The New Zealand Customs Service<br><br>The statistical information published by the government is currently divided across a number of reports which are issued by different agencies. During 2014–15, we met the Privacy Commissioner and the Deputy Privacy Commissioner and discussed opportunities for improving consistency and transparency in reporting.<br><br>We will continue to work with the Privacy Commissioner to explore options to increase the quality of public transparency and will update this section of the report in future if we have further information as a consequence of those discussions. | |

| Portugal | | |
|---|---|---|
| | Type of demand | |
| | Lawful Interception | Communications Data |
| Statistics | Government/other public body publishes (1) | 30,020 (2) |
| Key note (1) | The Portuguese government publishes statistical information related to lawful interception demands issued by agencies and authorities. | |
| Key note (2) | Prior to the 2014 report, the legal position was 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 were informed that we could disclose this information in the 2014 report. There has been no change to the guidance since that report: we have therefore updated this statistic with the latest information we hold for our own local operating business. | |

| 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) | Prior to the 2014 report, the legal position was unclear regarding whether or not it would be lawful for Vodafone to disclose statistics related to agency and authority communications data demands.<br><br>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.<br><br>We asked the authorities for guidance and were informed that we could not disclose this information in the 2014 report. There has been no change to the guidance since that report: we therefore cannot publish this information. | |

| Romania | | |
|---|---|---|
| | Type of demand | |
| | Lawful Interception | Communications Data |
| Statistics | Vodafone disclosure unlawful (1) | Unable to obtain guidance (2) |
| Key note (1) | It is unlawful to disclose any aspect of how lawful interception is conducted. | |
| Key note (2) | The legal position remains unclear regarding whether or not it would be lawful for Vodafone to disclose statistics related to agency and authority communications data demands.<br><br>Article 142(3) and Article 152 (3) of the Criminal Procedure Code (Law 135/2010) state that communication service providers are required to co-operate with criminal prosecution authorities with regards 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.<br><br>Prior to the publication of the 2014 report, we approached the authorities to ask for clarity and guidance as to whether Vodafone was lawfully permitted to disclose aggregate statistics related to communications data demands received from government agencies and authorities. We did not receive a response in time for publication of last year's report.<br><br>During 2014–15, we have again attempted to engage with the authorities to seek guidance but have again been unable to obtain clarity on the legal position. Given the uncertain legal position and the extent of potential risk to our employees associated with publication, we are therefore not in a position to disclose aggregate statistics related to communication data demands. | |

| 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 | 22,013 (1) | 43,537 (1) |
| Key note (1) | Prior to the 2014 report, the legal position was 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 were informed that we could disclose this information in the 2014 report. There has been no change to the guidance since that report: we have therefore updated these statistics with the latest information we hold for our own local operating business. | |

| Tanzania | | |
|---|---|---|
| | Type of demand | |
| | Lawful Interception | Communications Data |
| Statistics | No technical implementation (1) | 933 (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 number in the 2014 report (98,765) was mis-stated due to an administrative error in extracting the data from within our own operations. We have taken steps to address this process failure. | |

| 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 is conducted. | |

| United Kingdom | | |
|---|---|---|
| Type of demand | | |
| | **Lawful Interception** | **Communications Data** |
| **Statistics** | Vodafone disclosure unlawful (1)<br>Government/other public body publishes (2) | Government/other public body 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.<br><br>Note that in July 2014, the UK Government announced a review of the capabilities and powers required by law enforcement and security and intelligence agencies and the regulatory framework within which those capabilities and powers would be exercised. The UK's Independent Reviewer of Terrorism Legislation, David Anderson QC, was appointed by the Government to conduct the Investigatory Powers Review.<br><br>Vodafone met David Anderson QC and submitted its written evidence to the Review; a copy of that evidence can be accessed here.<br><br>The final report was published June 2015. | |

For a summary of the most important legal powers relating to law enforcement demands on a country-by-country basis, see our Law enforcement legal powers country-by-country annexe.