Law Enforcement Disclosure Statement

Digital Rights and Freedoms
Vodafone Group Plc

vodafone

Complex, controversial – and constantly changing

Communications technologies have evolved rapidly over the last 20 years. Almost three and a half 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. The telecommunications industry can be a tremendous force for social good, enabling people from all backgrounds and in all locations with the means to share, learn, innovate and enhance their lives and livelihoods.

With such advancements, and at such speed, it has become difficult for governments, agencies and authorities to keep pace with this dynamic and constantly changing industry. In many countries, the legislative framework determining lawful access by an agency or authority to citizens' private electronic communications was first defined in an era that predated the consumer internet. Our views on the legislative challenge that this presents for most countries (and for the telecommunications operators that provide the infrastructure) are set out later.

The use of legal powers in the context of today's complex electronic communications environment has proven to be highly controversial. In most countries, governments have incorporated national security exceptions into national legislation to provide agencies and authorities with powers to access private electronic communications. Some governments have chosen to constrain those powers to limit their impact on human rights or to apply a human rights test to the use of those powers. Others have not, preferring instead to equip agencies and authorities with wide-ranging powers that can have a substantially negative impact on human rights.

In a number of countries, these powers 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 and proportionality of state surveillance laws and practice.

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

However, in every country in which we operate, we also have to abide by the laws of those countries that require us to disclose information about our customers to law enforcement agencies or other government authorities. Those laws are designed to protect national security and public safety or to prevent or investigate crime and terrorism. 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.

Perceptions of the tension between privacy and security are not static; the underlying factors evolve constantly and are a regular topic in our conversations with a wide range of people and organisations including governments, privacy activists and NGOs, intelligence agencies, politicians and regulators. Over the past year, those discussions have helped us to form a view on the most appropriate approach to the many challenges in this area. We are grateful to all for their insights and suggestions, many of which we have tried to reflect this year.

Matthew Kirk
Group External Affairs Director
Vodafone Group Plc

[1] Source: 3.424 bn in 2016: http://www.internetlivestats.com/internet-users

What we are publishing and why

This is our third Law Enforcement Disclosure Statement in which we seek to offer some insights into the legal frameworks, governance principles and operating policies and procedures associated with responding to demands for assistance from law enforcement and intelligence agencies.

We continue to retain much of the explanatory text used when we published our first Law Enforcement Disclosure Report in July 2014 as our core principles and practices are unchanged. In addition, our explanation of the policies and processes we follow when responding to demands for assistance from agencies and authorities remains relevant and is repeated here.

The statistical information in this Statement covers the period from 1 April 2015 to 31 March 2016 with some additional commentary on events after that period. It encompasses the activities of our local market operating companies in 26 countries (including our joint ventures and associates) plus two other countries in which we have received a lawful demand for assistance from a law enforcement agency or government authority. We do not include 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.

We have updated the statistical information in our country-by-country section of this Statement for the two categories of law enforcement demands that we record: lawful interception and communications data demands. Those two categories account for the overwhelming majority of law enforcement demands received. We also explain the principles, policies and processes we follow when responding to agencies and authorities who demand our assistance with their law enforcement and intelligence-gathering activities.

We continue to disclose the aggregate number of demands we received during 2015-16 in the 28 countries encompassed by this Statement, 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). We also cite the relevant legislation that prevents us from publishing this information in certain countries.

We have also updated our Legal Annexe to include a country-by-country summary of the most important legal powers in force in our countries of operation. This year we have also included a new section within the Legal Annexe covering the current laws that relate to encryption and law enforcement assistance – the first time such an analysis has been published. The Legal Annexe also provides an update on the legal position in those countries that have new laws in force at the time this analysis was undertaken in the spring of 2016.

Compiling this disclosure remains complex and challenging, not least because in certain countries there are potential risks for our employees that 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 our original disclosure, we have tried to implement an approach that covers the 28 countries involved 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. Public attitudes on the appropriateness of intrusive surveillance measures can also vary greatly from one country to another.

This Statement remains the most comprehensive of its kind in the world. Other telecommunications operators have begun to produce similar disclosures in recent years, which we welcome. However, there is little consistency in the approach taken by different operators to the publication of statistical information. The cumulative effect of individual operator transparency reports is no substitute for comprehensive disclosure by governments with – ideally – independent oversight.

We recognise there are a number of other issues related to privacy and law enforcement that are not addressed here. Those issues can transform rapidly, beyond the timetable of a static annual publication. We have therefore created a new Vodafone *Digital Rights and Freedoms Reporting Centre* online, where we will post updates on the implementation of our policies, our views on new and emerging challenges in this area and our response to specific major events or themes related to the protection of our customers' private communications and the actions of the state to ensure public safety. We believe this continuous disclosure model – which replaces the 'moment in time' single Reports of 2014 and 2015 – will be of much greater benefit to the many stakeholders who follow these issues with interest. This Statement is now available in the *Digital Rights and Freedoms Reporting Centre* together with our views on other relevant topics including government-mandated network shutdowns and our Freedom of Expression Principles. During 2017-18, we intend to expand the range of opinions and disclosures available in the *Digital Rights and Freedoms Reporting Centre*.

The transparency challenge

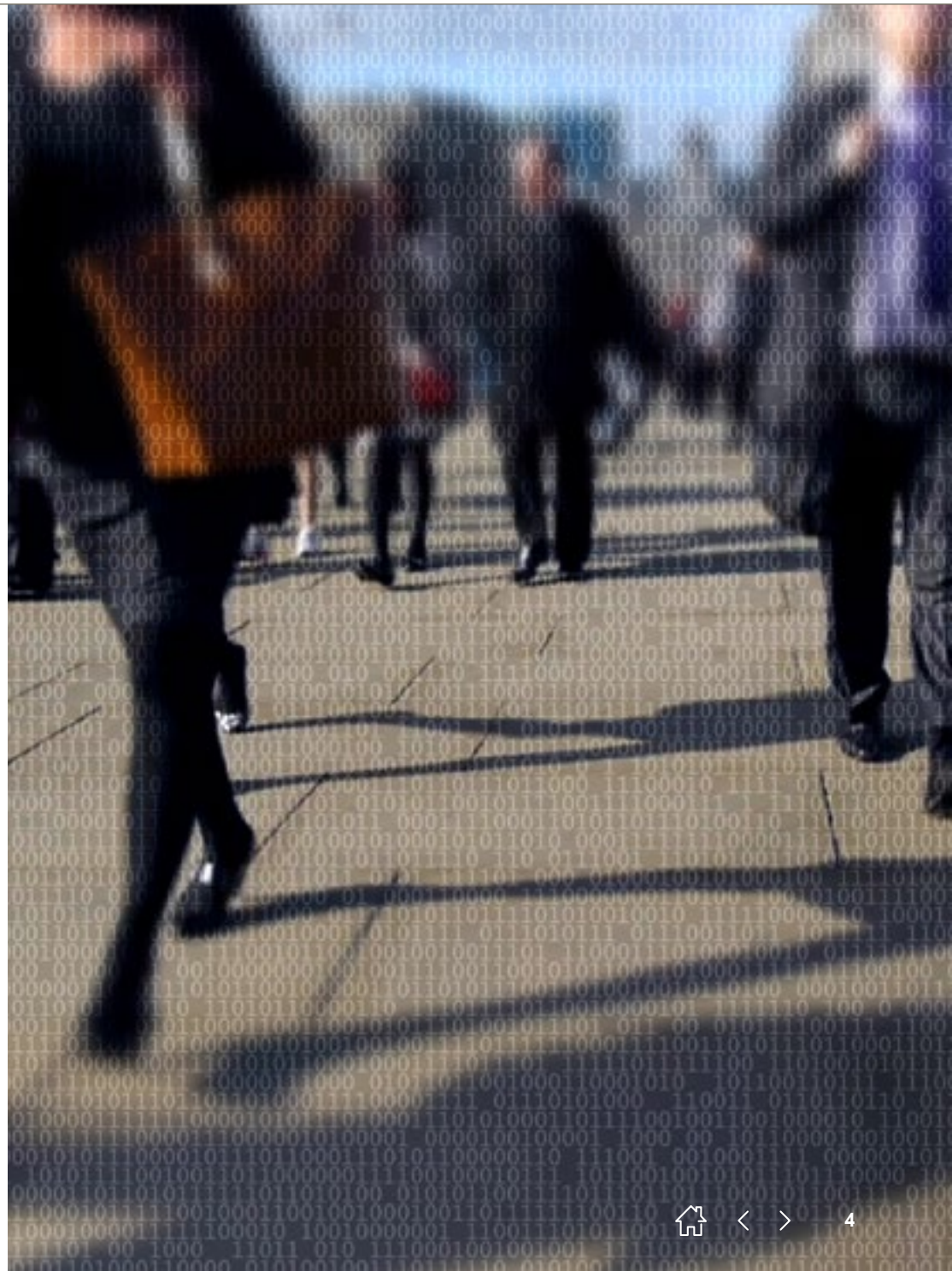
Law enforcement and national security legislation often includes stringent restrictions preventing operators from disclosing any information relating to agency and authority demands received, including disclosure of aggregate statistics.

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.

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 our Legal Annexe, we set out the laws and practices, on a country-by-country basis, that limit or prohibit disclosure, as 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 2016, we worked with Hogan Lovells to update the existing content of this Annexe for those countries that had new laws in force at the time the analysis was undertaken.

The Legal Annexe now also summarises the main laws relating to encryption in the context of law enforcement assistance in the telecommunications sector across 28 countries – the first time such an analysis has been published. We explain our views on encryption later.

In a number of countries, the law governing disclosure remains unclear; it can also be difficult to engage with the relevant authorities to discuss these issues. Where we are unable to obtain any clarity regarding the legality of disclosure, we have refrained from publishing any statistics. Where the government has informed us that we cannot publish statistical information held for our own operations, we have complied with that instruction in order to ensure that we do not put our employees at risk or risk the revocation of our licence to operate, which would prevent us from providing services to our customers. In a number of countries, we continue to try to engage with the authorities in order to seek opportunities 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 Statement 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.

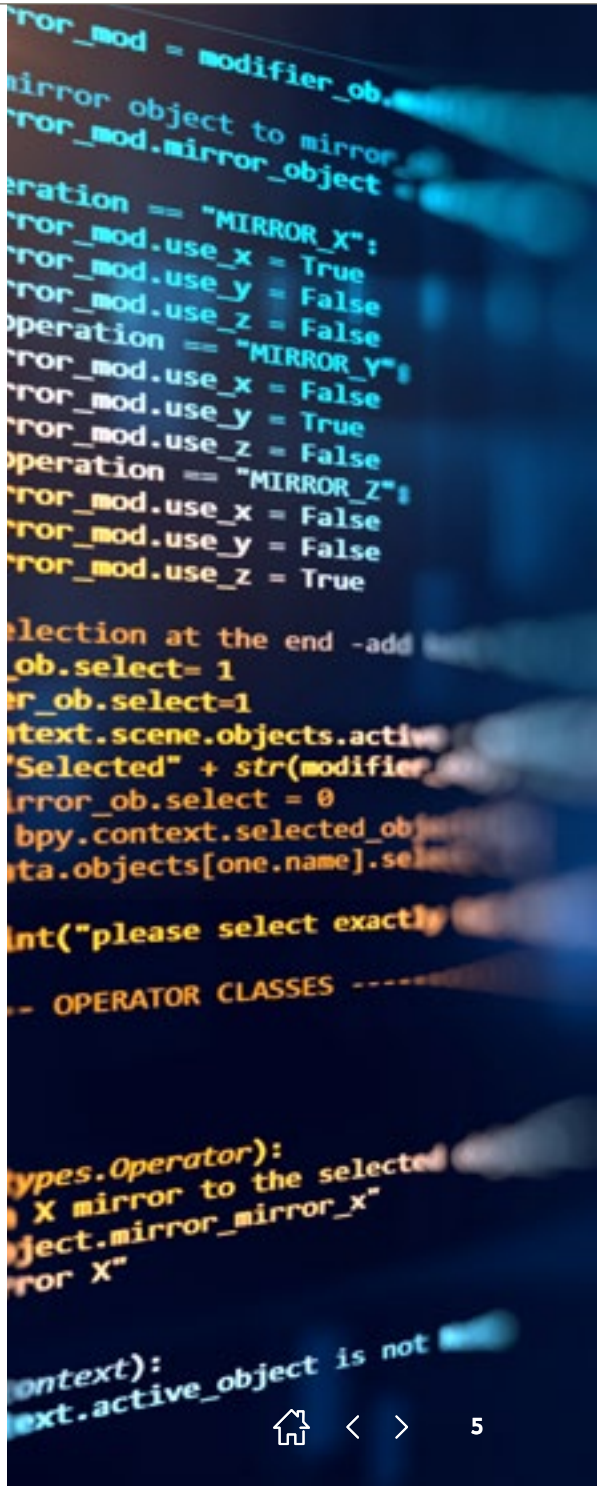
First, it is not possible for an individual operator to provide a full picture of the extent of agency and authority demands across a country as a whole, nor can an individual operator understand the context of the investigations generating those demands. Moreover, after several years of engagement with other telecommunications operators in many countries, we have concluded that a significant number of other companies would be unwilling or unable to commit to the kind of disclosures made by Vodafone.

Second, we have seen that, of those operators who do publish data in some form, each has widely differing approaches to the recording and reporting of 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 mix of all four) for their own operations. In addition, multiple different legal powers may be invoked to gain access to a single customer's communications data, which could legitimately be recorded and disclosed as either multiple or separate demands – or even one demand. Our views on the scope for considerable inconsistency in this area are explained below.

To add to the potential for confusion, an agency or authority might issue the same demand to different operators and each operator would then record and disclose the demand it received in its own way (with all of the variations in interpretation explained below). The result is that the cumulative number of all operators' disclosures would bear little resemblance to the fact that a single demand had 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.

We believe that 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 below 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).

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 2015-16. However, our concerns about the inadequacy of this kind of disclosure remain.

It is important to 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.

Finally, it should be made clear that a country with a surveillance regime operated without independent oversight that has minimal lawfully disclosable statistical information available cannot be compared favourably with another country whose checks and balances – including parliamentary and judicial oversight – produce disclosable statistics with warrants measured in the hundreds of thousands per year. It would be incorrect to conclude that the citizens of the latter country have less freedom than those of the former. Comparative numbers cannot and must not be relied upon to reveal meaningful truths.

What statistics should be reported: warrants or targets?

In the country-by-country section of this Statement, we have focused on the number of warrants (or broadly equivalent legal mechanism) issued to our local businesses, as we believe this is the most reliable and consistent measure of agency and authority activity currently available. The relatively small number of governments (nine 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.

As we have explained above, 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 it can 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. The scope for miscounting given all of the above is, therefore, immense.

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.

In our view, therefore, 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. This is, 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.

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 Statement 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 group of employees is tasked with liaising with agencies and authorities in order to process demands received. Those employees are usually security-cleared and are bound by strict national laws to maintain confidentiality regarding both the content of those demands and the methods used to meet them. The employees involved are not permitted to discuss any aspect of a demand received (or whether or not such 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 little or 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. In addition, 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.

While we have included factors relevant to national security powers in compiling this section, 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 of this Statement.

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'). We are a signatory to the Industry Dialogue's Guiding Principles on Freedom of Expression and Privacy, which define 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, principles and performance in these areas can be found in the new *Digital Rights and Freedoms Reporting Centre*.

As we explain in our Privacy and Law Enforcement Principles, 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.

Our core principle is that all demands received must conform to the requirements stated in law. For example, when our employees are told by the authorities that they must close down all or part of our network or shut down access to certain content or services, they will make it clear by reply that the appropriate written authorisation is required. Under certain circumstances – for example, a senior military officer demanding immediate constraints on communications networks in response to inter-communal violence – our insistence on respect for due process can put those employees at immediate and severe risk of harm. Despite that risk, wherever feasible and under most circumstances, our employees will tell the government representatives making the demand that the global policy of the Group is clear on these matter and – in the majority of cases – will subsequently receive the necessary written instruction. In all such instances, we work closely with the members of the Global Network Initiative to coordinate an industry-wide response. Further details of our views on network shutdowns and censorship are set out in our *Digital Rights and Freedoms Reporting Centre*.

Demands for assistance made by agencies or authorities acting beyond their jurisdiction will always be refused, in line with our Principles. In these cases the agency or authority in question would be told to pursue a government-to-government 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 three categories below.

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 Privacy 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.

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 that 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 that protects our customers and reduces the risks to our employees without compromising our principles.

The Vodafone Privacy and Law Enforcement Principles

We do not:

- allow any form of access to any customer data by any agency or authority unless we are legally obliged to do so;
- go beyond what is required under 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.

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 keep pace with new and developing technologies and services. In our view, those 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, smartphones and watches – 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 that 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; or, alternatively, 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 that 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 that govern how electronic communications networks must operate and that 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. In our Legal Annexe, we have therefore 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. The latest version includes an update on the legal position in 13 countries where new laws have come into force since our last Report was published (and at the point in time – the spring of 2016 – when this most recent analysis was conducted). It is worth noting that at the time of updating the existing content in the Legal Annexe, new laws were proposed or pending in several more of our countries of operation including Ghana, Hungary, Ireland, Lesotho, Malta, Mozambique, The Netherlands, South Africa, Turkey and the UK.

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'. 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. So, for example, an Italian agency can only seek lawful interception access to – or demand access to data held within – Vodafone Italy's networks.

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 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.

If an agency or authority wishes to demand access to communications data held abroad on another Vodafone network, they must initiate a MLAT request – on a demand-by-demand basis. A MLAT request 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 applicable privacy or data protection laws, and with the appropriate privacy and security safeguards in place, operators may also use communications data for business purposes.

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, a debate we follow closely. 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.

Data retention

Since our first report was published in 2014, the legitimacy of data retention law has been questioned in a number of countries where we operate. Most notably, the European Court of Justice has declared that the EU Data Retention Directive was unlawful and, more recently, it has reviewed subsequent challenges to Swedish and UK data retention law.

We have made it clear to all stakeholders – including governments – that we believe law enforcement powers (including data retention measures) must be balanced, proportionate and targeted and defined by the necessary, not the possible. If governments determine that data retention laws should apply on grounds of national security and shape legislation to this effect, then we are bound by the law.

We employ senior and experienced security and privacy experts in each country whose roles include ensuring that customer information is handled and stored in a safe and secure manner in line with our legal obligations. In a number of countries, independent oversight bodies also play a role in conducting external reviews of our policies and security controls to further provide assurance to customers.

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 content of communications 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.

The vast majority of countries empower agencies and authorities to require the disclosure by operators of the encryption 'keys' needed to decrypt data, an issue we cover in the new encryption section of our Legal Annexe. 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; this makes decrypting such data technologically impossible, regardless of what the law might be interpreted to say. We address the legal aspects of this issue in the new encryption section of our Legal Annexe. There is now 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. As we explain below, encryption will be a key topic for further discussion in 2017-18.

Encryption

Encryption plays a critical role in protecting our customers' private communications. In the near future, it will also play an equally vital role in securing the data that will be transmitted between billions of devices connected to the so-called 'Internet of Things'. Encryption is integral to the functioning of the global economy; modern society would cease to be viable in its current form without the ability to move funds and transmit confidential information securely across digital networks. Additionally, citizens' willingness to put digital networks and services at the centre of their daily lives depends in large part on their confidence that their privacy will be protected.

Encryption is now at the centre of one of the most complex and controversial debates in the history of the global telecommunications and technology industries. For many, encryption is a sacrosanct component of data security that underpins the individual's ability to seek and share information and opinions freely online. However, there is also a widespread view that the technologies that protect the public simultaneously enable individuals (such as criminals and terrorists) intent on causing public harm to conduct their activities out of sight of law enforcement and intelligence agencies.

Views are increasingly polarised and impassioned, driven by a belief that fundamental principles are at stake, ranging from the citizen's right to privacy and freedom of expression to the ability of the state to ensure public safety and the future of information security in the digital age.

Encryption makes it harder for unauthorised users such as hackers or fraudsters to access private data. There is therefore a clear benefit for society as a whole arising from the use of encryption to protect the security of lawful communications from unlawful interception. However, law enforcement and intelligence agencies in many countries are concerned that the reverse is also true: that encryption is being used to protect unlawful communications from lawful interception, making it more difficult to prevent crime and protect national security. Terrorists, child sex offenders and other criminals use the same communications technologies as the rest of society, and benefit from the same advances in privacy protection.

There is increasing anxiety within a wide range of stakeholder groups that a serious paradox is emerging: the technology that best protects the public is also putting the public at risk. Over the last two years, those concerns have been reflected in proposals for new legislation in a number of countries – proposals that have, in turn, led to growing concerns about the potential for serious unintended consequences, including increased risk of cyber attacks through weakened network integrity via decryption 'back doors' and a chilling effect on freedom of expression.

It is also likely that at some point in the near future when the majority of all internet traffic is end-to-end encrypted in some form, hackers and other unauthorised users will find ways to penetrate what are currently considered to be secure and trusted connections. Encryption technologies will need to continue to evolve rapidly to ensure effective protection for consumers, business and the public as a whole.

As we explain earlier, telecommunications operators are obliged to provide agencies and authorities with access to customers' private communications upon receipt of a lawful demand for assistance. However, if those private communications are encrypted and the operator has no means of providing agencies and authorities with the key, the agency serving the lawful demand would only achieve access to (at the most) a very limited set of metadata. The content of the communications would be unintelligible. As a result, there is now a growing tension between what is mandated in law and what is feasible in practice.

There is an urgent need for alignment between governments, law enforcement and intelligence agencies, civil society groups, digital rights activists, licensed telecommunications operators, internet companies and the public as a whole to agree on the way forward. As a first step – and to help to inform an ongoing debate – we have published an updated version of our Legal Annexe, which includes a summary of national laws regarding encryption and law enforcement assistance in the telecommunications sector in the 28 countries covered here – the first time such an analysis has been published. It is clear from this analysis that there is a significant degree of legal uncertainty regarding encryption and law enforcement powers in many of the countries in which we operate. In many countries there is no legal framework related to encryption and law enforcement whatsoever and the law does not always take into account what is now technically possible. This is a theme that we intend to explore further in 2017-18, with our views updated as required within the new *Digital Rights and Freedoms Reporting Centre*.

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.

Further details about the situation in each of the 28 countries we cover in this Statement are set out in our country-by-country section, where we disclose statistical information about the number of demands received wherever it is legal to publish this information and the authorities do not already do so themselves.

For our latest Legal Annexe click here and to access our *Digital Rights and Freedoms Reporting Centre* click here.