Freedom of Expression and Network Censorship

Digital Rights and Freedoms
Vodafone Group Plc

vodafone

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.

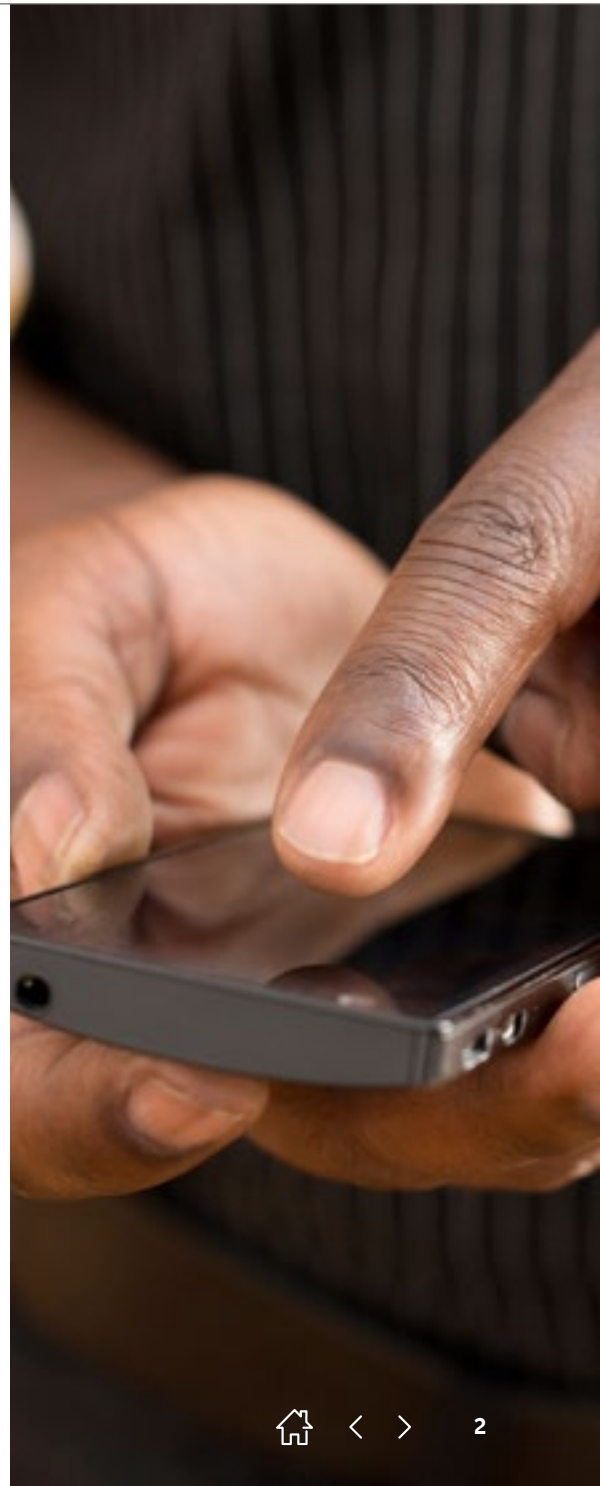
We are a significant investor in many of the countries in which we operate. Widespread prosperity is critical to the achievement of returns on those investments; businesses perform best under healthy macro-economic conditions with a large proportion of the population gainfully employed, earning and economically active. 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 make an investment, acquire a licence or operating company, or enter into a commercial relationship with a third-party operator in a country where Vodafone currently has no such presence.

All governments reserve the right, through legislation, to limit their citizens' ability to access and use digital networks, services and content under certain circumstances. In this Statement, we provide an overview of the challenges faced by telecommunications operators in seeking to respect their customers' right to freedom of expression. This includes a summary of 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.

We set out our 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 later. Those Principles should also be seen in the context of our Law Enforcement Disclosure Statement that offers a detailed insight into the relevant legal frameworks and Vodafone governance principles, operating policies and procedures in force across 28 countries.

Our Legal Annexe provides, on a country-by-country basis, an overview of the categories of legal powers used by governments, agencies and authorities to shut down or restrict access. The Annexe has been updated to include a new section covering the current laws related to encryption and law enforcement assistance in the telecommunications sector, as well as an update of the legal position in those countries that have new laws in force. Both the Law Enforcement Disclosure Statement and the Legal Annexe can be found in our new *Digital Rights and Freedoms Reporting Centre*, together with our Privacy Commitments, our statement of alignment with the Telecommunications Industry Dialogue Guiding Principles and our views and approach to the Digital Rights of the Child.



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 in our Law Enforcement Disclosure Statement), in practice their networks 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 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. The OTT companies' core business is providing advertising, 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 ever- 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 as this, in our view, is the area of greatest public concern and debate.

Service restrictions or network shutdowns

In our experience, government-mandated shutdowns of network or internet access ultimately harm the wider interests of the citizens that those governments are supposed to serve. However, our own beliefs and experience matter little when we receive a lawful order from the authorities to restrict our customers from using our networks (or the internet services provided over our networks). Ultimately, we have no choice but to comply with such an order: refusal would put our employees at risk of criminal sanction, including arrest and imprisonment. Despite that risk, wherever feasible we do seek to challenge orders or demands that appear to us to be overly broad, insufficiently targeted or disproportionate in nature, as we explain in our Freedom of Expression Principles on page 7.

In those Principles, we explain the very limited circumstances under which governments should be able to use their legal powers to require us or other telecommunications operators to block or restrict access to our networks or to online services. We also make clear our position on what governments should and should not do in this area. In our view, governments must ensure that national laws that interfere with freedom of expression must be 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.

In June 2016, the United Nations Human Rights Council (UNHRC) passed a landmark resolution stating that it 'condemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law'. The UNHRC specifically 'calls on all States to refrain from and cease such measures'.

We are a founding member of the Telecommunications Industry Dialogue on Freedom of Expression and Privacy (the 'Industry Dialogue') and are a signatory to their Guiding Principles which define a common approach to be taken by operators when dealing with demands from governments, agencies or authorities that may affect customers' privacy and freedom of expression. The Industry Dialogue works in partnership with the Global Network Initiative (GNI), an international NGO that brings together internet, telecommunications and information technology companies, civil society groups including human rights and media freedom activists, academics and investors. The GNI's mission is to develop a common approach to protecting and advancing free expression and privacy around the world. In February 2016, the GNI announced a closer alignment with members of the Industry Dialogue under which Vodafone became an observer member. One year on, in March 2017, Vodafone became a full member of the GNI Board.

The Industry Dialogue and GNI's joint position on network and internet access shutdowns is as follows: 'The protection of national security and public safety are important government concerns. Network shutdowns, and the wholesale blocking of internet services, however, are drastic measures that often risk being disproportionate in their impact. Governments who employ these measures often do so without justifying them as necessary and proportionate under international human rights standards.'

The most salient powers available to governments to block or restrict access to communications services 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 that grant additional powers (under national security legislation) to agencies and authorities engaged in national security matters that 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 that 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. For more information on our approach to protecting children from inappropriate content click here.

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, a topic we cover in more detail here. 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. The Industry Dialogue and the GNI published a joint statement on network shutdowns in 2016.

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, even more so when the order enabling the use of these powers is constantly renewed over an extended period. These powers 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.

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 state of internet freedom around the world

Freedom House is an independent organisation dedicated to the expansion of freedom and democracy around the world. Its report, *Silencing the Messenger: Communication Apps Under Pressure*, reveals that, in an international context, internet freedom declined for the sixth consecutive year in 2016.

Analysis of the laws and agency practices in the 65 countries assessed by Freedom House reveals that two-thirds of all internet users live in jurisdictions where criticism of the government, military or ruling family is subject to censorship.

More governments than ever before are targeting social media and communication apps as a means of halting the rapid dissemination of information, particularly during anti-government protests. Governments' efforts to control internet-based communications underline the key role these technologies play in facilitating political discourse and – within repressive regimes – enabling individual citizens to share information and address matters of social injustice.

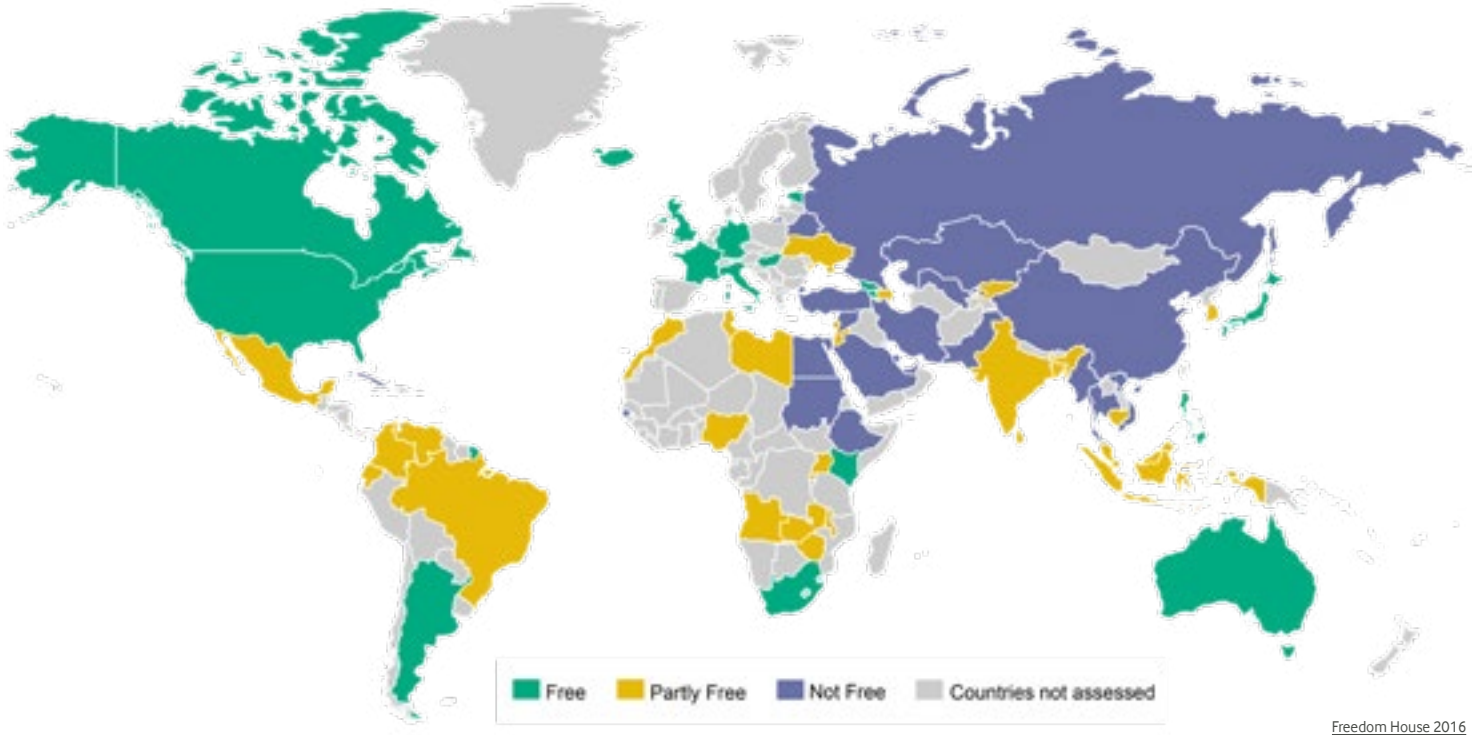
Online activism is a critical contributor to the advancement of human rights. In more than two-thirds of the countries covered in the Freedom House study, online activism has produced a wide range of direct outcomes, from the defeat of a restrictive legislative proposal to the exposure of corruption through citizen journalism.

Governments in a number of countries have resorted to a total shutdown of all internet access during periods of political tension in order to prevent their citizens from disseminating information that the government deems to be hostile towards it.

Those shutdowns can have significantly adverse social, economic and human rights consequences as companies, public sector, emergency services and healthcare providers are unable to exchange the information needed to manage their organisations effectively. Governments also increasingly seek to block or censor online content that represents a challenge to their authority or their view of acceptable social norms. Sites and pages blocked include those used to initiate digital petitions, call for public protests, communicate the views of political opposition groups or address LGBT+ (lesbian, gay, bisexual, transgender and other forms of sexuality and gender identity) issues. In countries with a history of authoritarian rule, the authorities have also used new national security and anti-terrorism legislation as a means of limiting their citizens' right to privacy and ability to freely express their opinions on topics such as democratic representation and minority rights.

To read the full Freedom House report, click here.

The State of Internet Freedom Globally



Freedom House 2016

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

The Vodafone Freedom of Expression Principles

We do:

- respect and seek to protect our customers' 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[1]; 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.

1 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.

How access to communications are blocked or restricted

There are a range of different methodologies that telecommunications operators can use when they are 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 in our Freedom of Expression Principles.

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, governments, agencies and authorities are becoming increasingly concerned that blocking and filtering technologies are becoming less effective as a consequence. For more information on our views on encryption, see our Law Enforcement Disclosure Statement.

Statistical information

Research conducted by Vodafone in 2015 concluded that it was not possible for Vodafone to present a meaningful statistical analysis of government efforts to block or restrict access to services or content. We worked with our colleagues across 26 countries to look at:

- 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.

Our conclusion then was that publication of this data is not possible. That remains the case today.

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 variable and disjointed. Numbers alone can provide no meaningful insight into the extent to which the citizens of one country benefit from greater freedom of expression than those of another. For example, a statistical methodology that recorded every instance that online content was blocked in a particular country on grounds that it contained unlawful images could produce public records measured in the thousands every year. Would the citizens of that country be less at liberty to exercise their right to freedom of expression than those in a country whose government passed just one order in the year that blocked an entire category of content accessed daily by millions of people?

We believe statistics should be treated with great caution, for reasons we explain in more detail in our Law Enforcement Disclosure Statement.

In our view, the obligations for governments to publish this information at least annually (as we explain in our Freedom of Expression Principles) 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.