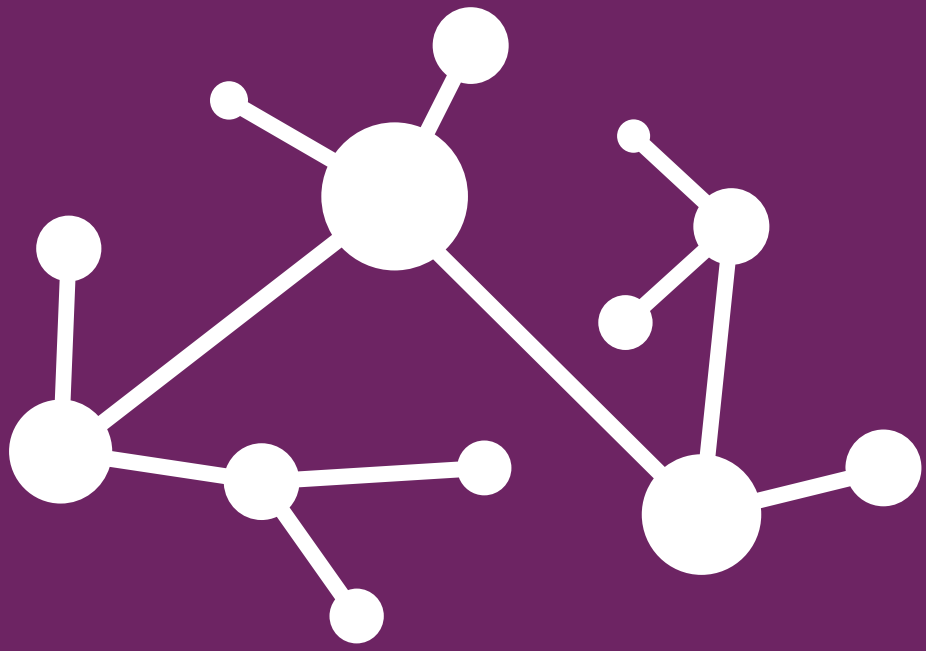
ARTICLE 19



# Getting connected: Freedom of expression, telcos and ISPs

June 2017

Policy Brief

**ARTICLE 19**
Free Word Centre
60 Farringdon Road
London,
EC1R 3GA
United Kingdom
T: +44 20 7324 2500
F: +44 20 7490 0566
E: info@article19.org
W: www.article19.org
Tw: @article19org
Fb: facebook.com/article19org



The Principles were developed as a part of the Civic Space Initiative financed by the Swedish International Development Cooperation, Sida. Sida does not necessarily share the opinions here within expressed. ARTICLE 19 bears the sole responsibility for the content of the document.

# Executive Summary

In this policy, ARTICLE 19 examines the obligations of telecommunications (telcos) and Internet service providers (ISPs) to protect and respect human rights, in particular the right to freedom of expression, and to remedy violations of these rights.

ARTICLE 19 considers that the extent of telcos and ISPs' responsibilities with regards to human rights reflect the critical role these businesses play in enabling individuals to exercise their right to freedom of expression. This policy brief explores the contours of these responsibilities. Our starting point is the UN Guiding Principles on Business and Human Rights (the Guiding Principles), which require telcos and ISPs to integrate human rights safeguards and mitigate human rights impacts.

We recommend that, in order to ensure that telcos and ISPs comply with their responsibilities with regards to human rights, in particular with the Guiding Principles, telcos and ISPs should ensure that in their operations, they embody the fundamental principles of a human rights-based approach, namely:

- **Respect for human rights**: terms of service should be publicly available and accessible, formulated with sufficient precision to enable users to understand their implications and regulate their conduct accordingly, and restrict users' exercise of human rights only where necessary to achieve a legitimate aim and where proportionate to that aim;

- **Participation**: users should have the right to participate in decisions that implicate their human rights. Terms of service should be based on obtaining users' express free and informed consent, and should guarantee that users will be notified of measures that will infringe upon their human rights;

- **Empowerment**: users should be sufficiently informed and empowered to engage with terms of service and contest them under certain circumstances. Users should have control over their personal information in a manner that is consistent with the right to freedom of expression;

- **Non-discrimination and equality**: Internet users should enjoy non-discriminatory access to the Internet, their online content and data should be treated equally and without discrimination;

- **Accountability**: terms of service should be transparent and clear about the conditions under which users' human rights will be restricted. In particular, terms of service should disclose how and under what conditions telcos and ISPs will respond to government orders and requests for disclosure of personal data. Terms of service should provide an effective remedy for individuals to contest such decisions.

The policy also provides detailed recommendations on specific measures that are deployed by telcos and ISPs – either at the behest of, or under compulsion by, the State (including network shutdowns, state surveillance, the generation and retention of certain data, or bans on particular applications or services) or voluntarily, in some cases driven by commercial interests. Specific recommendations addressing how the private sector should bring such practices into line with international human rights law are set out.



# Table of contents

# Introduction

Access to the Internet – as well as digital connectivity more broadly[1] – is no longer the preserve of the fortunate and better-off, but rather has become an essential requirement for all, regardless of economic or educational status. It is through digital technologies that a 21st century population learns, earns, acts and transacts, and exercises a range of human rights, in particular the rights to freedom of expression and information, assembly and association, and education[2]. Digital technologies have also become the medium through which States deliver a range of social and public services. As a result, some argue that the Internet – its backbone of key protocols and infrastructure - can be considered a global public good that provides benefits to everyone in the world[3].

Although States bear many obligations with regards to the Internet, access to it is, in most circumstances, mediated by private actors. Telecommunications companies (telcos) and Internet service providers (ISPs) (jointly, providers) connect individuals with the complex infrastructure of wires, cables and satellites that enable them to "go online." Moreover, emerging community providers represent an alternative form of digital inclusion, play an important role in diversifying the Internet access pool and contribute to plurality and diversity of Internet connection models. Providers act as a gateway between individuals and their enjoyment of human rights, and play a critical role in enabling people to access public services and connect to the world's information.

Providers frequently take measures, at the behest of governments, which threaten individuals' human rights. These include shutting down networks, restricting the use of certain services and applications, facilitating the punitive disconnection of access for copyright infringement, facilitating government surveillance, and prohibiting encryption and anonymity online. Emerging changes and challenges, from the advent of 5G networks to intensifying debates about law enforcement access to encrypted devices, raise the stakes even higher.

Increasingly, we are also witnessing providers taking measures, in the name of compliance with their terms of service (also called "terms and conditions"), which undermine and imperil human rights, including the right to freedom of expression and information. These measures include unilateral actions such as restricting access to online content, generating, retaining and selling users' personal information, and prioritising certain types of content based on its origin, destination or service provider.



Compounding the asymmetry of power between providers and users is the lack of transparency around, and accountability for, how terms of service are interpreted and applied. Lengthy, complex and legalistic language obscures the intent of terms of service, and the "one-way" nature of the relationship between providers and users inhibits genuine scrutiny or negotiation of the terms of that relationship. Under most terms of service, individuals are rarely entitled to contest, or even be informed of, adverse decisions by providers to, for example, facilitate government surveillance, disclose data to third parties, undermine network neutrality or disconnect access. Terms of service are often a black box that - under the guise of having users consenting to it - obfuscates, rather than illuminates, the role of providers and their contractual obligations towards their users.

ARTICLE 19 believes that understanding the role and responsibilities of private actors is key to protecting freedom of expression and information, as well as other human rights online. Hence, this policy brief explores the contours of those responsibilities. Our starting point is the UN Guiding Principles on Business and Human Rights (the Guiding Principles), also known as the Ruggie Principles, which require providers to integrate human rights safeguards and mitigate human rights impacts in their operations, and to publish transparency reports and provide effective remedies for human rights violations. We recommend that, in order to ensure compliance with the Guiding Principles, providers should establish terms of service that embody the fundamental principles of a human rights-based approach, based on respect for human rights, participation, empowerment, equality and accountability.

**The scope of this policy**

A complex web of actors constitutes the sector responsible for building, providing and maintaining the physical and technical components that make up the Internet and ensure connectivity. For the purposes of ascribing responsibilities regarding the rights to freedom of expression and information, ARTICLE 19 has suggested that these private actors can be divided into the following categories:[4]

- **Actors providing essential services in order to gain access to the Internet:** these include telecommunications companies, telcos, Internet access providers, network operators, and Internet exchange points;

- **Actors providing essential services in order to gain access to information on the internet:** these include ICANN, domain name registries and registrars, web hosting services, and search engines;

- **Actors who facilitate the sharing of information on the Internet:** these include social media sharing platforms, blogs, online forums and e-commerce services offering or distributing content;

- **Actors producing content:** this includes newspapers and other content producers, whether individual authors or companies;

- **Other actors:** including computer or other hardware manufacturers, software developers, companies providing data storage or cloud services, and cyber-security firms, who are essential for providing network security.

We could also describe these actors as providing services on the **physical layer**, the **logical layer**, the **content layer**, and the **social layer** of the Internet, respectively. Policy discussions pertinent to protection of human rights, including the right to freedom of expression, permeate all four layers; while policy changes on one layer will have a direct impact on the others, in some form or fashion[5.]

In this policy, we focus on telcos and ISPs, the private or State-owned entities that provide and maintain the technical layer of the Internet, providing individuals with access to the Internet via mobile or fixed-line services. The policy applies to both commercial and community providers.

Because of the complexity and scope of this issue alone, we do not address here private sector entities that host content (such as web hosting providers) or those that provide services and applications online (such as social media platforms or messaging apps). We also exclude content delivery networks (CDNs), Internet exchange points (IXPs), and other entities whose clients are companies, rather than individuals; as well as the range of other private actors whose actions have implications for freedom of expression in the digital context, including hardware manufacturers and software developers, content producers and copyright holders, companies providing data storage or cloud services, or cyber-security firms. These are being addressed in separate ARTICLE 19 policies.

This policy builds upon previous work by ARTICLE 19 that addressed the roles and responsibilities of intermediaries in the context of freedom of expression and information online;[6] and it also provides specific recommendations for both States and providers in the respective areas of this policy.



# Applicable international standards

The telecommunications sector has evolved in markedly different ways across countries and contexts. In many places, telecommunications were initially state-owned monopolies, which have now become fully or partly privatised, and telecommunications markets have been opened up to new and foreign actors[7]. In other contexts, the telecommunications sector has always been a fully privatised endeavour.[8]

However, States still own interests in many telcos around the world and, even in fully privatised markets, the legacy of State ownership and the regulatory role of the State, continues to characterise the close relationship between telcos and governments. This relationship is also informed by the framework for telecommunications licensing, which requires telcos to comply with government-stipulated conditions in order to operate.

ISPs are more likely to be private actors, having emerged with the birth of the Internet to provide so-called "last mile connectivity": linking individual users with existing telecommunications infrastructure. Whereas there is less likely to be a legacy of State ownership or influence over ISPs, in many countries ISPs operate as monopolies due to a lack of competition. In some contexts, including in rural or poor communities, the lack of commercial incentives for ISPs to operate sees the obligation to provide "last mile connectivity" fall to the State. Recently, we have seen the emergence of community service providers[9] that are diversifying the opportunities to access the Internet.

All providers – whether State-owned, private or community – have responsibilities to respect and protect the human rights of Internet users, in particular the rights to freedom of expression and information and to privacy. These responsibilities, as elaborated under the Guiding Principles, include positive duties to mitigate adverse human rights impacts, publish transparency reports and enable avenues of redress.

## The right to freedom of expression and information

The right to freedom of expression is guaranteed in Article 19 of the Universal Declaration of Human Rights (UDHR), in the International Covenant on Civil and Political Rights (ICCPR) as well as in regional treaties.[10] It encapsulates a right not only to impart, but also to seek and receive, information and ideas of all kinds, regardless of frontiers; the right to access information is increasingly accepted under international law as an integral part of the right to freedom of expression.[11] In recent years, numerous international bodies and instruments have confirmed that the right to freedom of expression must be protected online as it is protected offline.[12]

The right to access the Internet is not explicitly recognised as such under current international and regional human rights law. However, developments in certain national laws, together with developments in international and regional human rights law, are moving towards urging all States to enable access to the Internet for all[13]. Access to the Internet has also been recognised as inextricably linked to the exercise of freedom of expression, as the UN Special Rapporteur on freedom of expression and opinion (Special Rapporteur on FOE) noted in his 2011 report:

> [T]he access to information, the ability to exercise the right to freedom of expression and the participation that the Internet provides to all sectors of society is essential for a truly democratic society.[14]

The right to freedom of expression is not absolute and may be curtailed in accordance with strict conditions. Permissible limitations on free expression are set out in the so-called "three part test", which requires that all restrictions:

- Are **provided by law**;
- Pursue a **legitimate aim** – exhaustively provided for in Article 19 para 3 of the ICCPR to include: (a) respect of the rights or reputations of others; or (b) the protection of national security or of public order *(ordre public)*, or of public health or morals; and
- Are **necessary and proportionate** to that aim.[15]

These permissible limitations apply equally to restrictions on freedom of expression which take place online. Importantly, the question of proportionality takes on greater weight in the online context since, due to the nature of the Internet, any restrictions on human rights have the potential to affect hundreds of millions of Internet users. Assessing whether a particular restrictive measure, which affects the Internet, amounts to a violation of human rights standards thus requires a nuanced understanding of the technical and practical implications for freedom of expression and privacy, and recognition of the cross-jurisdictional impacts of restrictions on access to online services and content.

In their 2011 Joint Declaration on Freedom of Expression and the Internet, four special mandates on freedom of expression[16] emphasised that, in the context of access to the Internet, compliance with the permissible limitations test implies, among other things, that:

- Measures to **block** particular websites, services or uses, or to **deny individuals the right to access the Internet**, are extreme measures which must meet the strict requirements of the three-part permissible limitations test;
- There should be no **discrimination** in the treatment of Internet data and traffic based on the device, content, author, origin and/or destination of the content, service or application;
- Internet intermediaries should be **transparent** about any traffic or information management practices they employ, and relevant information on such practices should be made available in a form that is accessible to all; and
- **Cutting off access** to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified, including on public order or national security grounds.

In June 2016, the UN Human Rights Council (HRC), in response to a number of States having recently shut down access to the Internet or digital communication tools, unequivocally condemned

> [M]easures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law and call[ed] on all States to refrain from and cease such measures.[17]

The HRC's strongly-worded statement reflected the severity of the impact of network shutdowns on the enjoyment of the right to freedom of expression. Although the resolution does not elaborate upon when restriction or disruption of Internet access will violate international law, the UN Human Rights Committee (HR Committee), which oversees compliance of signatories with the provisions of the ICCPR, has previously stipulated that wholesale bans on sites or tools will amount to a violation:

> Any restrictions on the operation of websites, blogs or any other Internet-based, electronic or other such information dissemination system, including systems to support such communication, such as Internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government.[18]

## The right to privacy

The right to freedom of expression is closely connected with the right to privacy, in particular in the context of the Internet. Privacy acts as a shield to ensure that individuals can share ideas and seek information online without being subjected to arbitrary and unlawful surveillance, monitoring and data collection, ensuring they can exercise their free speech rights confidentially and, if they so choose, anonymously. In this way, the right to privacy functions to create the conditions necessary for the free and full enjoyment of freedom of expression and information online.

The right to privacy, enshrined in Article 12 of the UDHR and Article 17 of the ICCPR and in regional treaties,[19] forbids unlawful interference with an individual's privacy, home, correspondence and family. As the Internet and digital technologies have evolved, understandings of privacy have expanded to include an individual's personal data, with protection of personal data having been derived from the right to privacy.

**Protection of personal data**

The first international statement on the scope of the right to protection of personal data was the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which has since been complemented by the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (known as Convention 108)[20], the 1990 UN General Assembly Guidelines for the Regulation of Computerized Personal Data Files,[21] and the European Union's Data Protection Directive, recently upgraded and replaced by the General Data Protection Regulation.



Today there are more than 100 national data privacy laws around the world, nearly half of which are from outside Europe, [22] and many of which closely replicate European standards. The European Court of Human Rights and the Court of Justice of the European Union (CJEU) have been at the forefront of articulating the contours of the right to protection of personal data as it relates to privacy.[23] Regional instruments addressing this issue have also been adopted by the Association of Southeast Asian Nations (ASEAN) and the African Union.[24]

The right to privacy is not an absolute right; it can be restricted subject to the same, aforementioned, three part test applicable to freedom of expression.[25] As such, activities which interfere with individuals' privacy, such as the targeted surveillance of online communications or the generation, collection, retention and use of personal data, may be justified provided they are in accordance with the law, necessary to meet a particular objective, and proportionate to that objective.

In the context of activities that involve the generation, collection, retention and use of personal data online, data protection law[26] prescribes restrictions and safeguards to ensure that data processing does not infringe upon Internet users' right to privacy. Although data protection regulation differs across countries and regions, all data protection laws have common principles which pertain to the processing of personal data online:

- **Fairness and lawfulness:** this includes the obligation to obtain the informed consent of an individual prior to processing their personal data;
- **Purpose limitation:** data should be collected for specific, explicit and legitimate purposes, and not used for other incompatible purposes;
- **Data minimisation**: data should be limited to what is necessary, and be adequate and relevant;
- **Accuracy:** personal data should be accurate and up to date;
- **Storage limitation**: identifiable personal data should not be kept for longer than is necessary;
- **Security and integrity:** organisations should adopt appropriate organisational or technical measures to ensure that stored data is secure;
- **Accountability and transparency:** organisations should be transparent about how they are processing data and accountable for abiding by data protection principles.[27]

## The private sector's responsibilities

There now exists considerable guidance, in the form of the HR Committee General Comments and Concluding Observations, Special Rapporteurs' reports, and the jurisprudence of regional courts, regarding the responsibilities of States in the context of the protection of the right to freedom of expression and information on the Internet.[28] However, there remain comparatively few materials articulating the responsibilities of those private actors who maintain and provide Internet access, and who very often act to facilitate State interference in access to the Internet.

A notable exception are two reports by the Special Rapporteur on FOE, including his 2017 report to the HRC which analysed the role and responsibilities of the Internet access sector in promoting the right to freedom of expression.[29] The report elaborates upon the friction that arises when ISP's domestic legal obligations conflict with international human rights law, particularly in the context of network shutdowns, content blocking, copyright enforcement, communications surveillance, and interference with net neutrality. The Special Rapporteur on FOE focussed on the duties of States to respect freedom of expression in the context of two particularly severe interferences, network shutdowns and communications surveillance, as well as States' duties to ensure freedom of expression by banning paid prioritisation and regulating zero rated services. He then went on to explore the contours of corporate accountability in this context, fleshing out the obligations of private sector actors to conduct due diligence, embrace human rights safeguards by design, build leverage, adopt mitigation strategies, publish transparency reports and ensure effective remedies are in place.

The framework established in the **Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework** [30] (the Guiding Principles) – alongside the earlier Ten Principles of the UN Global Compact,[31] – provides a starting point for articulating the role of the private sector with regards to human rights and the Internet.[32] The Guiding Principles recognise the responsibility of business enterprises to respect human rights, independent of State obligations or the implementation of those obligations, by:

- Making a **public statement of commitment** to respect human rights, endorsed by senior or executive-level management;
- Conducting **due diligence and human rights impact assessments** in order to identify, prevent and mitigate potential negative human rights impacts of a company's operations;
- Incorporating human rights **safeguards by design** in order to mitigate adverse impacts, and building leverage and acting collectively in order to strengthen power vis-a-vis government authorities;
- Tracking and communicating **performance, risks and government demands**; and
- Making **remedies available** when adverse human rights impacts are caused.

Some work has been done to apply the Guiding Principles to the specific circumstances of telcos and ISPs. Notably, in 2013 the Telecommunications Industry Dialogue (TID) developed its own set of Guiding Principles to inform the internal policies and processes of its members.[33] The Global Network Initiative (GNI), which focuses more on Internet companies and intermediaries than telecommunications companies, also issued its own Principles,[34] which the Ranking Digital Rights Corporate Accountability Index uses – along with the UN Guiding Principles – to rank the performance of Internet and telecommunication companies on a yearly basis.[35]

Whereas the TID and GNI Principles focus primarily on providing guidance to companies as to how they should respond to government demands, the Ranking Digital Rights (RDR) looks at the obligations of ISPs when it comes to terms of service. RDR prescribes a set of indicators to assist in assessing companies' adherence to human rights principles. These indicators include, *inter alia*:

- The availability of terms of service and privacy policies;
- Notification of changes to terms of service and of restrictions to content or access;
- What information is disclosed in the terms of service, such as:
    - Whether the company prohibits certain types of content or activities;
    - Under what circumstances the company may restrict services to users;
    - What process the company employs to evaluate and respond to requests from governments to restrict content or services;
    - What user information the company collects, with whom they share it, and for how long they keep it;

- Whether the Internet user has control over the data the company collects and shares;
- Whether the Internet user can access all of the information the company holds about them;
- Publication of transparency reports about government and private requests to remove, filter or restrict content or access, or to provide access to stored data or real-time communications;
- Publication of data about the volume and nature of actions taken to enforce terms of service;
- Publication of data about network management;
- Whether the company notifies Internet users when their data has been requested by governments and other third parties; and
- Whether the company deploys industry standards of encryption and security, and permits users to encrypt their content.[36]

These indicators, whilst not exhaustive and fully comprehensive, provide important baseline guidance for ensuring that terms of service take into account, and do not undermine, Internet users' rights to freedom of expression and privacy.



# Measures that undermine users' human rights

A range of measures deployed by telcos and ISPs seriously threaten individuals' rights to freedom of expression and privacy. Some of these measures are taken at the behest of, or under legal compulsion from, the State: such measures include network shutdowns, state surveillance, the generation and retention of certain data, or bans on particular applications or services. Other measures are taken voluntarily, including those driven by commercial interests: the generation and analysis of excessive amounts of personal data, for example, or the implementation of paid prioritisation schemes. In this section, we analyse the practices taken by telcos and ISPs that have implications for human rights. Specific recommendations as to how the private sector should bring such practices in line with international human rights law are addressed in the following section.

## Withdrawal of access

**Network shutdowns**

The centrality of the Internet to the exercise of freedom of expression in the modern era has increased the appeal to States of using network-wide shutdowns to suppress access to, and dissemination of, progressive and dissenting information and ideas. As a result, the frequency of full and partial network shutdowns, particularly during elections[37] and other times of political upheaval, has increased significantly in recent years.[38] Shutdowns have also been used during university entrance exams under the auspices of preventing student cheating and during protests and demonstrations[40] to prevent individuals from accessing mobile and Internet communications.

Network shutdowns are given effect by providers, acting at the behest – and often in response to the direct demands – of States. In some circumstances such demands are grounded in domestic legislative frameworks, such as those pertaining to emergencies and threats to national security,[41] while in others States apply pressure to, or request the cooperation of, providers to shut down networks in the absence of any applicable regulation. Regardless of the existence of domestic legislation purporting to authorise network shutdowns, however, blanket measures of this type are never permissible under international human rights law.[42]

**Graduated response laws**

Since 2009, numerous countries have adopted punitive laws and policies designed to penalise repeat infringers of copyright law through the disconnection of their Internet access. Graduated response laws, also known as "three strikes and you're out" laws, involve telecommunications companies withdrawing Internet access to users responsible for multiple copyright infringements.[43] In some circumstances, providers voluntarily comply with such regimes, disconnecting users' Internet access in the absence of executive or judicial orders.[44]

When Internet access is such a central enabling condition for the enjoyment of human rights, withdrawing individuals' access becomes a punitive and serious interference with the right to freedom of expression and other human rights. As a result, it cannot be deemed to be proportionate under international human rights law, regardless of the justification advanced.[45]

## Restrictions on access

Providers restrict, interfere with and discriminate against the network traffic they handle in a variety of different ways. A narrow category of such restrictions is justified by reference to network management, which necessitates prioritising some network traffic for the effective governance of network flows. However, a range of other measures see content, applications and services being prioritised, throttled or blocked. These include:

- **Paid prioritisation**, a revenue-raising measure which sees providers accepting payments from platforms and service providers to prioritise content on the basis of origin, destination or service provider, delivering some categories of Internet content at higher speeds, while deliberately slowing or throttling other categories.

- **Zero-rating arrangements**, whereby providers offer access to certain content or services for free and restrict access to other content or services. Although such arrangements are billed as providing access to under-served communities who might not otherwise be able to afford Internet access, they have the effect of curtailing the content users are able to access, stymieing the free flow of information and shutting users off in "walled gardens."[46] Some argue that zero-rating is "only suited for scenarios where bandwidth is extremely expensive or where demand for bandwidth far exceeds supply, and zero-rating is used to incentivize lower bandwidth usage;" but even in such situations should avoid the harms of distorting content consumption, freedom of expression and privacy, access to markets and other harms.[47] Hence, providing unfettered access to the full Internet is a better solution than zero-rating to certain content.



- **Bans on applications and services:** in numerous countries, applications such as Voice over IP[48] or instant messaging apps,[49] and services such as Virtual Private Networks[50] are made unavailable by providers, either voluntarily or at the behest of governments.

Each of these measures violate an early and fundamental pillar of the open Internet, that of network neutrality. Net neutrality (or content agnosticism[51]) holds that network traffic – the "packets" which carry content across the Internet – should not be treated differently based on their origin, destination, or service provider, or on the basis of the kind of service or application. Ensuring network neutrality means that providers cannot use their control over Internet infrastructure to block, slow or prioritise access to content from certain origins or providers, to certain kinds of content, or to certain applications or services.

Net neutrality is a key prerequisite to ensuring the equal and non-discriminatory exercise of the rights to freedom of expression and information. Without it, there is no longer an even playing field online, and the capacity of individual users to determine how they engage with online content and applications is severely undermined. Measures to undermine net neutrality also threaten the right to privacy and data protection, as giving effect to prioritisation schemes may involve providers subjecting network traffic to a more invasive level of scrutiny using, for example, deep packet inspection.

Net neutrality is also threatened by the impending roll-out of 5G, the next generation of mobile Internet connection, and the vastly expanded capabilities 5G will enable. Because 5G networks will be able to meet an incredibly diverse set of needs, the risk that providers will choose to create "fast lanes" for certain types of content, treat some data packets with priority, or throttle bandwidth is increased.[52] In July 2016, some of the world's largest telcos signed a 5G Manifesto[53] calling into question the necessity of net neutrality standards, raising fears that free expression rights will be subjugated to network efficiency considerations.[54]

Because they interfere with the rights to freedom of expression and information, for measures that violate network neutrality to be compliant with international human rights standards they must satisfy the permissible limitations test. In this regard, the measures articulated above raise a number of concerns:

- **Legality:** Not only are paid prioritisation schemes and zero-rating arrangements not provided for by law, they are often prohibited by domestic regulation. A number of countries have banned zero-rating services,[55] or

have enacted domestic law requiring zero-rated services to refrain from unreasonably interfering with users' ability to access content freely.[56] In November 2015, the European Union adopted rules on net neutrality that prohibit blocking, throttling or discrimination with regards to online content, applications and services, save for certain exceptions: compliance with legal obligations, integrity of the network, and congestion management in exceptional and temporary situations.[57]

In countries where bans on particular applications or services are part of domestic law, such laws must be publicly available, and sufficiently clear and precise. Vague laws or broad references to various justifications (often national security) must not be used to enforce bans on specific applications or services.

- **Necessary to meet a legitimate objective and proportionate to that objective:** Restrictions on access to particular online content, applications and services are unlikely to be justifiably necessary to ensure either respect of the rights or reputations of others, or for the protection of public order or morals. It is feasible that some prioritisation of network content may be justifiable in exceptional situations of urgency, for example a major national security or public health emergency. In such circumstances, however, in order to be proportionate restrictions on access would need to be temporary and limited to what is strictly required for the duration of the emergency.

## Generation, retention and disclosure of data

Providers are situated at a unique point in the communications value chain, one which potentially gives them insight into extraordinary amounts of information about their users, from identifying data collected when accounts are initiated to billing data; from geo-location information logged when users access a service, to the details of the websites they visit and applications they use; from the size and type of content users download to the content of text messages and, in some cases, emails. As such, telcos and ISPs handle an extensive amount of highly private and personal data about their users.

A certain amount of access to personal data by providers is necessary, of course for billing subscription users, for example, or for connecting Internet users with particular websites. However, the large majority of data that providers handle need only be retained momentarily, there being no traffic management determinants for its long-term retention.



Nevertheless, with the increasing commercialisation of personal data, telcos are discovering the financial benefits of generating, collecting and retaining large swathes of personal data that are not essential for the delivery of the service, but which, put together, enable companies to create monetisable user profiles. The onward sale of use of personal data to third parties may see individuals' personal data being shared widely with advertising companies and data brokers. Where telcos offer free services, such as public wifi networks, they may collect even more data, and share such data not only with corporate entities but with States.

States are also alive to the value of personal data to law enforcement and intelligence agencies, and are placing increasingly onerous obligations on telecommunications providers to generate and retain personal data on subscribers, their communications and the websites and applications[58] they access to facilitate government surveillance objectives. Mandatory data retention laws, requiring providers to generate and store communications data records for up to two years, can now be found in countries across the world.[59] Real name registration policies, requiring providers to record and verify the identity of users of even pre-paid services, are also proliferating.

Data about an individual's use of the Internet – "metadata" – can be just as sensitive as the content of their communications. For this reason, there is increasing judicial recognition that metadata deserves the same legal protections as that applicable to content. The Inter-American Court of Human Rights has confirmed as much in the context of telephone calls, stating:

> [The right to privacy] applies to telephone conversations irrespective of their content and can even include both the technical operations designed to record this content by taping it and listening to it, or any other element of the communication process; for example, the destination or origin of the calls that are made, the identity of the speakers, the frequency, time and duration of the calls, aspects that can be verified without the need to record the content of the call by taping the conversation. In brief, the protection of privacy is manifested in the right that individuals other than those conversing may not illegally obtain information on the content of the telephone conversations or other aspects inherent in the communication process, such as those mentioned.[60]

As the CJEU has noted, the data handled by telecommunications companies, taken as a whole,

> [i]s liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, that data provides the means […] of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications.
>
> The interference entailed by such legislation […] raises questions relating to compatibility not only with [the rights to privacy and protection of personal data] but also with the freedom of expression […].[61]

Where States impose requirements on providers to generate and retain data, those requirements will not comply with international human rights law where they amount to blanket measures, which are "neither necessary nor proportionate."[62] The CJEU has stipulated that compliance with the rights to privacy and freedom of expression necessitates the State to establish a link between the data to be retained and the specific objective to be pursued, and limit the retention of data to specific time periods, crimes or geographic locations.[63]

Beyond State-imposed data retention, providers should limit the amount of personal data they require from and store about their users, including for the purpose of advertising. Doing so would heighten Internet users' sense of privacy and empower them to exercise their free expression rights unhindered by the fear of monitoring. Moreover, it would ensure providers are able to meet their obligations under data protection law, which requires companies to minimise the amount of data they collect, and delete identifiable personal data once it is no longer necessary. Moreover, companies are not permitted to use the data they collect for one purpose – such as facilitating Internet users' access to messaging applications – for another incompatible purpose, like advertising, without first gaining the individual user's informed consent.



## Facilitating state surveillance

Although telecommunications providers have long acted as a go-between for government surveillance, the scope, diversity and gravity of modern day surveillance dwarfs previous interception programmes. Whereas postal mail interception and landline wiretaps may have seen telcos facilitating State access to a small percentage of personal correspondence and phone calls, today providers are the conduit through which almost all the world's communication, commerce, information, and knowledge travel. As computing power advances, storage costs plummet and governments' surveillance ambitions grow ever greater, providers are being asked – in some cases, forced – to operate and expedite a global monitoring apparatus, in many cases in violation of international human rights standards.

In addition to complying with requests for access to personal and communications data and content (addressed above), there are a number of means through which telcos facilitate government surveillance:

- Retrofitting telecommunications infrastructure or removing protections from infrastructure to enable State surveillance;
- Installing State surveillance equipment directly onto telecommunications infrastructure; and
- Permitting States to have direct access to, or control over, telecommunications infrastructure for the purposes of surveillance.

While surveillance by government authorities may be a justifiable interference with human rights, it must comply with the permissible limitations test. In the context of telecommunications surveillance, the following considerations are relevant:

- **Legality**: Whereas surveillance measures must have a basis in both domestic law, and be compliant with the rule of law, in many countries surveillance is a completely unregulated endeavour, or fails to meet requirements regarding the quality of law. Surveillance laws must be sufficiently clear and precise to enable individuals an adequate indication of the circumstances in which their communications may be intercepted and monitored.[64] They must also indicate the scope of the discretion granted to the executive or the judge empowered to order surveillance, and be accompanied by specific safeguards.[65]

- **Necessary to meet a legitimate objective and proportionate to that objective:** Because international human rights instruments do not prescribe an exclusive list of objectives for which surveillance may be legitimately conducted, human rights focuses instead on the safeguards in place to prevent against abuse of surveillance laws, such as laws which specify authorisation and oversight processes, and limits on the duration of surveillance.[66] Authorisations should be targeted, issued by an independent judicial authority, and subject to the existence of a reasonable suspicion against the person concerned.[67]

Satisfying the proportionality test requires an examination of whether it would have been possible to achieve the objective by less intrusive means. It also requires taking into account the human rights impact of the measure; in the context of surveillance measures, which affect potentially hundreds of millions of users of particular network, the proportionality test will often fail to be satisfied.



# Remedies for human rights violations

Despite being considered a key pillar of the Guiding Principles, the responsibilities of the private sector to provide access to effective remedies is often neglected in policy-making. Indeed, providing an effective remedy for human rights violations has been called "the forgotten pillar" of the Guiding Principles' framework. Moreover, the Guiding Principles focus primarily on the State's duty to facilitate remediation, and, as a result, thinking on the responsibilities of the private sector in this regard remains underdeveloped.

Some recommendations have been developed by civil society organisations. For example Access Now's Telco Remedy Plan outlines the procedural and substantive aspects of remedy in the context of telcos.[68] The Remedy Plan builds on more general guidance from organisations such as the Council of Europe[69] and the European Commission ICT Sector Guide on Implementing the Guiding Principles on Business and Human Rights[70] and speaks specifically to the procedural and substantive steps that telcos and ISPs should take in order to enable remediation for violations of the human rights of Internet users. It asserts that telcos should introduce a broad range of measures, in particular:

**Procedural measures**

- Incorporate the question of remedy into due diligence with the help of all stakeholders before entering new markets or offering new services in existing markets;

- Seek to implement grievance mechanisms that are accessible and secure for complainants;

- Respond quickly and effectively to complaints brought to company grievance mechanisms;

**Substantive measures**

- Investigate and find ways to cease or alter activities that contribute to adverse human rights impacts in an effective, timely manner;

- Interview executives and staff overseeing and conducting those rights-infringing activities, and review relevant policies. Clarify whether staff deviated from policy or the policy itself failed. To minimise the risks of repetition, revise policies, retrain staff and communicate policy changes to personnel, business partners and the public;

- Preserve evidence wherever possible and publish when appropriate, particularly when obstacles make providing access to effective remedy impossible in the near-term. In cases where the state instigated the telco's rights-infringing activities, evidence can inform a victim's search for effective remedy, especially where states deny their role in unlawful surveillance, censorship or network interference;

- After consulting those affected, acknowledge and apologise as appropriate for any contributions to human rights abuses. In many cases, apologies and assurances of non-repetition can go a long way towards remedying the telco's contribution to the harm the victims suffered;

- Submit to independent investigation or ongoing oversight conducted independently of the telco, and with full access to corporate officials and records. Inquiries should proceed transparently, to a publicly available deadline and in coordination with multiple stakeholders, including civil society, legal and regulatory experts, and government officials. Ongoing oversight is required when the same form of infringement has occurred repeatedly or when the infringement is determined to be the result of systemic problems within the company;

- Organise and participate in regional or sector-wide entities, with structured multi-stakeholder participation, to clarify and mitigate any role telcos play in systemic human rights violations. These bodies should adhere to best practices in transparency and accountability, to be determined and updated in consultation with other stakeholders and according to regular, publicly available timetables. Policy changes and other outcomes should likewise be coordinated and evaluated against established benchmarks;

- Compensate victims and affected communities. Compensation as a remedy for human rights abuses has become comprehensible in light of the International Criminal Court's "Trust Fund for Victims". If the telco sector established such a fund, it could benefit from sector-wide backing, both financial and moral, and draw on the vast expertise of the world's largest telcos, foundations, governments, investors, and civil society stakeholders.

The principles articulated above, although not comprehensive, provide a robust foundation for beginning a discussion on the responsibilities of telcos and ISPs to provide victims of human rights violations with an effective remedy. When applied to the most common human rights-infringing measures committed by telcos and ISPs, ARTICLE 19 believes that compliance with these principles requires providers to take several steps to remedy the violations of freedom of expression (see the final section).

# ARTICLE 19's recommendations

## General recommendations

ARTICLE 19 suggests that providers should adopt a human rights-based approach to their operations, embodying the following principles and recommendations. We also recommend that providers should take part in and explore supporting self-regulatory initiatives to monitor and promote human rights in compliance with these recommendations.

**Recommendation 1: Compliance with international human rights principles**

**Telcos and ISPs should ensure that their operations are consistent with internationally-recognised human rights standards. Where local laws and State demands conflict with those standards, providers should seek to comply with international human rights principles to the greatest extent possible.**

Providers should not act on any state orders that manifestly interfere with human rights unless such orders are issued by an independent judicial authority, and should exhaust all available remedies to challenge them. Working collaboratively with peer companies to challenge demands, and engaging with the public and civil society about such demands, may increase providers' leverage. It is critical that providers implement any State orders in a manner that minimises the impact on individual end users.

Wherever possible, providers should publish information about requests or orders issued by States that interfere with human rights. If providers are placed under secrecy obligations, they should consider adopting innovative approaches such as warrant canaries (a method where providers are able to inform their users if they have not been served with government orders to facilitate surveillance) to give individuals an indication of the existence of requests or orders.

Providers should actively resist any requests or orders that would wrest control of telecommunications infrastructure away from the provider and put it in the hands of the government. This includes, for example, government demands to provide direct access to providers' infrastructure. Providers should go to all feasible lengths to prevent this eventuality.



Providers should advance innovative measures to enhance individuals' rights, in particular the rights to freedom of expression and privacy, even if such measures frustrate or prevent State requests and demands. This includes applying advanced encryption to telecommunications networks, and minimising the data collected and retained in order to minimise the risk of forced disclosure.

**Recommendation 2: Ensuring clarity and accessibility**

**Providers' terms of service should be publicly available and accessible, and formulated with sufficient precision to enable individuals to understand their implications and regulate their conduct accordingly.**

Terms of service should be written in clear language and should not hide behind obscure references to compliance with local laws. They should explicitly list the relevant legislation with which the telco must comply and they should forecast for the individual the circumstances under which the telco may be subject to State requests or demands that would impact upon an individual's rights to freedom of expression or privacy. Providers should explore innovative ways to communicate the impact of terms of service for their users, including using iconography, images and interactive explanation of their content.

Terms of service should commit providers to compliance with international human rights principles to the greatest extent possible. They should assure individuals that providers will challenge State requests and demands for withdrawal of access, restriction of services and applications, access to personal data and cooperation in state surveillance.

Terms of service should assure individuals that the provider will never disconnect individuals' access to the Internet as a voluntary or punitive measure.

Individuals should be able to access the providers' terms of service in a free and easy manner; it should be accessible in a range of formats that take into account differences in literacy, education, age and capacity.  Terms of service should use plain language wherever possible.

**Recommendation 3: Participation**

**Terms of service should give individuals the right to participate in decisions that affect their human rights**

Terms of service should be based on obtaining individuals' informed and express consent. In this regard, terms of service should require an explicit, non-ambiguous indication of the individuals' consent to the terms of the relationship with the telco. Consent to the use, generation, analysis and retention of personal data for certain purposes only applies to the purposes that the provider has directly disclosed to the individual. When the telco wants to collect more personal data, or use existing data in a different and inconsistent way, they need to obtain fresh informed consent and not rely solely on the primary/initial one.

Terms of service should guarantee individuals will be notified of measures that will impact upon their human rights. In this regard, terms of service should inform individuals of the circumstances under which they will not be notified, for example where gag orders might exist in the context of surveillance.

**Recommendation 4: Individuals' empowerment**

**Individuals should be sufficiently informed and empowered to engage with terms of service and contest them under certain circumstances.**

Terms of service should indicate to individuals where they have the right to challenge the terms of the relationship and how they can do so. Individuals should be informed about what grievance and remediation mechanisms are available to enable complaints regarding and requesting changes to terms of service.

Terms of service should inform individuals of their right, at any time, to access all of the personal data that providers hold on them, and to request the amendment or deletion of that data by the telco as well as by the subsidiaries with whom the data might have been shared as part of any agreement. Individuals should have the right to export personal data in an open and accessible format.

Providers should support digital literacy initiatives designed to educate Internet users about how to best protect the security and privacy of their information online and thus facilitate the empowerment of users. They should also engage in an industry-wide cooperation on data portability standards, to ensure that switching between providers is an easily attainable and implementable reality for users.



**Recommendation 5: Non-discrimination and equality**

**Terms of service should guarantee individuals will receive access to content, applications and services without discrimination.**

Network neutrality should be guaranteed in terms of service. Providers should guarantee individuals that they will not discriminate against communications content on the basis of origin, destination or service provider, or restrict in any way the content, applications or services an individual can access, except in the case of recognised exceptions and where necessary for traffic management. Free services should not be conditioned on restricted access to content, applications or services.

Terms of service should indicate to individuals where the provider is subject to judicial orders to restrict content, applications or services, and that individuals will be notified immediately if such an order is received. Terms of service should forewarn users about the potential use of gag orders and the measures the telco has put in place to supersede them, such as warrant canaries.

Acceptable measures for the purpose of network management should be explained to the individual in a manner that is clear and digestible. Individual users should be able to take part in independent and transparent monitoring processes that ensure that network neutrality is respected.

Providers should publish regular transparency reports including the details of any orders to which the telco is subject in accordance with which access to certain content, applications or services is restricted. Providers should also publish, on at least an annual basis, information about network management practices.

**Recommendation 6: Accountability**

**In terms of service, providers should be clear and transparent about the conditions under which individuals' human rights will be restricted. In particular, terms of service should disclose how and under what conditions providers will respond to government demands. Terms of service should provide an avenue for individuals to contest such decisions.**

Terms of service should state explicitly the circumstances that may lead to an infringement of individuals' freedom of expression and privacy rights. They should state the conditions under which the provider will accept or accede to State requests and demands. They should also indicate how individuals can access

information about the types and numbers of requests and demands to which the provider has been subject, and with which it has complied.

Terms of service should set out in detail how individuals can access grievance and remediation mechanisms to complain about or contest the telco's adherence to its terms of service.

## Specific recommendations

**Recommendations on network shut-downs**
In the face of requests or demands to facilitate measures which clearly violate human rights standards, providers have a responsibility to respect international human rights principles to the greatest extent possible.[71] This implies a responsibility to take the following steps with regards to network shutdowns:[72]

### Preparation and forecasting

- Identify domestic laws that could be used to order network shutdowns;
- Consult local civil society actors, peer companies and other sources of information to identify situations in which the State is likely to order a network shutdown;
- Educate staff about the possibility of a network shutdown and devise a decision-making strategy, including a public communications strategy, to be used in the event of a shutdown;

### Resistance strategies

- Seek clarification from the government as to the intention, duration and scope of the shutdown;
- Exhaust domestic remedies to challenge the relevant order, including by employing legal challenges before judicial authorities;
- Coordinate responses with peers in order to increase leverage;

### Mitigation and communication

- Identify potentially affected individuals and communicate to them the fact of the shutdown, its projected duration and scope, and provide them avenues for obtaining further information;
- Maintain control of the provider's infrastructure throughout the process;
- Stage and limit the shutdown (geographically and temporally) to the greatest extent possible;
- Restore access as soon as possible.



Terms of services should clearly state the conditions under which individuals' access to the Internet will be withdrawn as a result of a State-imposed network shutdown. In particular, in their terms of service providers should commit to:

- Not giving effect to network shutdowns unless all domestic avenues for challenging the shutdown have been exhausted;
- Notifying individuals immediately of a forthcoming shutdown and regularly providing them with up-to-date information about the shutdown; and
- Providing individuals grievance and remediation mechanisms to remedy any negative impacts of the shutdown that the telco is in a position to address.

**Recommendations on graduate response laws**
Providers' terms of services should indicate to individuals whether a graduated response law applies in their country of operation, and should clearly state the conditions under which individuals' access will be withdrawn pursuant to such laws.

In their terms of service providers should commit to:

- Never disconnecting an individual's access to the Internet as a voluntary or punitive measure;
- Only disconnecting an individual's Internet access if a disconnection order is issued by an independent judicial authority;
- Notifying an individual immediately if a disconnection order is received;
- Challenging the disconnection order on behalf of the individual until all domestic avenues been exhausted.

**Recommendations on net neutrality**
Providers must refrain from voluntarily applying measures that violate the principle of network neutrality. Where they are under a legal obligation to restrict access to particular services or applications, they must do so in a manner that ensures their compliance with international human rights principles to the greatest extent possible. In this regard, providers' terms of service should commit them to:

- Not discriminating against, or prioritising, content on the basis of origin, destination or service provider, or kind of application or service;
- Not restricting in any way the content, applications or services a user can access, except for the purpose of network management, and restricting such prioritisation to what is strictly required;
- Not conditioning the provision of free services on restricted access to content, applications or services;

- Only restricting access to content, applications or services where an order is issued by an independent judicial authority;
- Notifying users immediately if such an order is received;
- Challenging such orders until all domestic avenues been exhausted;
- Publishing, on a regular basis, details of any orders to which the telco is subject in accordance with which access to certain content, applications or services is restricted;
- Publishing, on a regular basis, information about network management practices;
- Submitting to independent external monitoring of traffic management measures and explain to users how they can take part in these processes;
- Refrain from using traffic management measures that invade privacy (such as deep packet inspection).

Providers could, however, consider "positive" alternatives to zero-rating, such as offering free access with monthly data caps. They could also encourage third party service providers to offer versions of their services with more efficient data usage to all Internet users (for example using better compression, lower audio bitrate and/or lower video resolution).

**Recommendations on data protection**

Providers should use their terms of services to clearly and explicitly communicate with individuals regarding what personal data is required from them, and generated, collected and stored about them. They should commit to:

- Always obtaining an individual's informed consent when using their personal data for a new or incompatible purpose;
- Requiring individuals to disclose the minimum amount of personal data necessary for provision of telecommunications access;
- Informing individuals about how their personal data is used, how long it is retained for, and with whom it is shared;
- Deleting identifiable personal data as soon as it is no longer necessary to provide access to the individual;
- Enabling individuals to access and review, at any time, the personal data held by the telco and the purposes to which it is being put;
- Enabling individuals to withdraw consent at any time for the processing of their personal data;
- Ensuring that personal data is protected by state-of-the-art organisational and technical security measures;
- Notifying individuals immediately if mandatory data retention orders are received;



- Notifying individuals immediately if requests for access to subscriber data, or communications data or content are received;
- Challenging such orders on behalf of the individual until all domestic avenues been exhausted;
- Notifying individuals if their personal data is disclosed to a government authority or another third party;
- Publishing, on a regular basis, details of any orders to which the telco is subject in accordance with which data is generated, retained or disclosed;
- Publishing, on a regular basis, information about personal and communications data and content which is being disclosed to government authorities or other third parties;
- Providing individuals with a grievance or remediation mechanism to contest disclosures of personal data in violation of the terms of service.

**Recommendations on surveillance**

Although some requests or demands for providers' assistance with State surveillance may be justified, providers are best able to ensure they meet their responsibilities to protect and promote human rights if they resist any requests or orders which would wrest control of telecommunications infrastructure away from the provider and put it in the hands of the government. Acquiescence to such requests creates a dangerous precedent, inducing an expectation on the part of the State that the telco will continue to modify its products and services in accordance with the State's preferences. Over-compliance should be avoided in all circumstances.

Providers should also advance innovative measures to enhance individuals' free expression and privacy rights, even if such measures frustrate or prevent State surveillance objectives. This includes, chiefly, applying advanced encryption to telecommunications networks.

Providers should communicate to their users in their terms of service how they will respond to State requests and demands to facilitate surveillance. This information should be full and frank, and not hide behind generic references to compliance with local laws. Providers should commit to:

- Robustly scrutinising any request or demand from States to retrofit or modify existing telecommunications infrastructure, or install surveillance capabilities;
- Exhausting all available remedies to challenge any request or demand to retrofit or modify infrastructure or install surveillance capabilities;
- Actively resisting, including by using public pressure, collective action and threats of market withdrawal, any request or demand by States for direct access to telecommunications networks;

- Publishing information, to the greatest extent possible, about any measures taken to retrofit or modify infrastructure or install surveillance or provide direct access;
- Wherever feasible, notifying individual users of specific surveillance measures to which they have been subject;
- Providing a grievance or mediation mechanism to enable individuals to challenge the providers' decision to comply with requests or demands.

**Recommendations on remedies**
Telcos and ISPs should ensure that there are grievance and remediation mechanisms in place to address negative impacts of their actions that the provider is in a position to remedy.

Robust **transparency practices** might provide a form of a remedial action[73] by providing the affected users with the right to be heard about the impact of the infringement on their lives. Moreover, the provision of information to affected users concerning the nature, scope and origin of human rights violations may empower them. In the context of network shutdowns, for example, informing users with regular and ongoing updates will place them in a stronger position to mitigate the negative effects of the shutdown.

In the case of serious and systematic State demands to facilitate human rights abuses, telcos and ISPs should consider whether compliance with international human rights standards could be best achieved through the **cessation of business operations** in a particular country or context.

The withdrawal of operations is a remedy which may itself undermine the human rights of Internet users; it may deprive users of connectivity on a temporary or permanent basis, increase the costs of connectivity, and facilitate the growth of monopolistic markets. However, where telcos are repeatedly placed under government pressure to facilitate serious human rights infringements, in particular surveillance and network shutdowns, the harm caused to users through such infringements arguably outweighs the harm of withdrawal.

In such circumstances, telcos should undertake a comprehensive assessment, in consultation with stakeholders, of the necessity, effects and potential impact on users of ceasing business activities in the relevant country. Decisions to cease business operations should be taken as a last resort and only after consultation with other sector entities about the possibility of leveraging collective action against the relevant government.



Additionally, telcos and ISPs should consider the following specific remedial actions:

For shutdowns
- Provide full and complete information, by all effective means, on the existence and extent of the shutdown, and, where feasible, on the existence of alternative access solutions (and the implications of the use of any such alternative access solution);
- Immediately restore network connectivity at the earliest available opportunity;
- Invite and record the accounts of users, enabling those whose connectivity was restricted to explain and document their experiences of the shutdown;
- Consider extending account credits or promotions as a form of universal compensation or altering bill payment periods;
- Take steps to compensate individuals who suffered demonstrable financial loss or substantial harm as a result of the shutdown; and
- Immediately convene a sector-wide discussion to contemplate how to leverage collective action against further government-imposed shutdowns.

For graduate response laws
- Immediately restore connectivity to the affected individual at the earliest available opportunity, either after successfully challenging the disconnection order or after the expiration of the disconnection period; and
- Take steps to compensate individuals who suffered demonstrable financial loss or substantial harm as a result of the disconnection.

For net neutrality
- Apologise to users and provide full and comprehensive information about the measures taken by the telco to prioritise, discriminate against or restrict particular content;
- Provide assurances to users that their future access to the network will not be subject to prioritisation, discrimination or restriction;
- Adopt transparency measures going forward to enable independent oversight of network management measures; and
- Support individuals to bring legal action to seek remediation or compensation from the responsible State.

For breach of data protection

- Provide affected users with full and comprehensive information about the personal data generated, retained and disclosed about them;
- Provide guarantees that personal data has been deleted and that any third parties to whom personal data has been disclosed have been requested to delete the data; and
- Take steps to compensate individuals who suffered demonstrable financial loss or substantial harm as a result of the generation, retention and disclosure of personal data.

For surveillance

- Notify the affected user, and provide full and comprehensive information about the type and scope of surveillance to which they were subjected;
- Invite and record the accounts of affected users, enabling them to explain and document their experiences of the surveillance;
- Take steps to compensate individuals who suffered demonstrable financial loss or substantial harm as a result of the surveillance; and
- Support individuals to bring legal action to seek remediation or compensation from the responsible State, including by challenging the legality of surveillance where appropriate.



# About ARTICLE 19

ARTICLE 19 is an international human rights organisation, founded in 1987, which defends and promotes freedom of expression and right to information worldwide.

It takes its mandate from the Universal Declaration of Human Rights, which guarantees the right to freedom of expression and information. An increasingly important means of expression and to seek, receive, and impart information is through information and communication technologies such as the Internet. ARTICLE 19 has been promoting Internet freedoms for over 10 years and is active in developments of policy and practice concerning freedom of expression and the Internet through our network of partners, associates and expert contacts.

ARTICLE 19 encourages organisations and individuals to give us feedback about how this policy brief is being used. Please send your feedback to legal@article19.org.

*This publication is wholly or partially financed by the Government of Sweden. The Government of Sweden does not necessarily share the opinions herein expressed. ARTICLE 19 bears the sole responsibility for the content.*

# References


1. The importance of mobile phones extends far beyond one to one communication; for example, in Global South, mobile telephony has played an important role in promoting democratic accountability, providing access to information, and propagating effective national campaigns; see, e.g. ARTICLE 19, Kenya: Free expression standards should guide fight against "counterfeit" mobile phones, 11 October 2011.
2. See, e.g. Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, A/HRC/32/L.20, adopted on 27 June 2016.
3. See, e.g., Persbericht WRR, Policy Brief No. 2: The public core of the internet: an international agenda for internet governance, 10 April 2015; or Jacob Kastrenakes, Obama says FCC should reclassify Internet as a utility, The Verge, 10 November 2014.
4. See ARTICLE 19, Freedom of expression and the private sector in the digital age: Submission to the UN Special Rapporteur, 2016.
5. C.Cath, N. ten Oever & D O'Maley, Media Development in the Digital Age: Five Ways to Engage in Internet Governance, March 2016.
6. These include, in particular the following ARTICLE 19 policies:
   - Internet Intermediaries: Dilemma of Liability (August 2013) which focuses on the models of liability applicable to actors operating on the content layer (such as web hosting providers) and the social layer (such as online platforms) of the Internet;
   - Freedom of Expression Unfiltered: How blocking and filtering affect free speech (December 2016) which examines the compatibility of blocking and filtering online content with international standards, and provides recommendations to governments and companies;
   - Policy Brief: The Right to Be Forgotten (March 2016) which provides comprehensive recommendations on how to ensure protection of the right to freedom of expression with regard to the so-called "right to be forgotten;"
   - The Global Principles on Freedom of Expression and Privacy (March 2017) that provide a systematic analytical framework for assessing how freedom of expression and privacy are mutually reinforcing, and determining the limits that can be placed on both rights when they are in conflict, online and off;
   - Policy Brief: ICANN's Corporate Responsibility to Respect Human Rights (October 2015) which sets out the reasons that the UN Guiding Principles on Business and Human Rights (UNGPs) are the most appropriate framework for ICANN to follow in its mission to develop human rights policies and processes, and then presents options as to how ICANN can begin to implement them.
7. E.g., the British Telecom, the world's oldest telecommunications company, was initially transferred to state control under the Post Office and later became a privatised company, the forerunner of BT Group Plc; see, e.g. BT, Origins of the BT. In Brazil, Telecommunications Code of 1963 established a state-granted monopoly, followed by the creation of Embratel in 1965 and the subsequent organization of the Telebras system in 1972 with a host of regional telecoms, Embratel (responsible for interstate and international calls) and CPqD (an R&D unit); see A.Musacchio & S.G.Lazzarin, State-Owned Enterprises in Brazil: History and Lessons, OECD, 2014.
8. E.g. in the USA; see R. W. Lucky & J. Eisenberg, The Evolution of the U.S. Telecommunications Industry and Effects on Research, NPA, 2016.
9. See, e.g. ARTICLE 19, Brazil: ARTICLE 19 launches guide on community internet providers, 19 January 2017.
10. The European Convention on Human Rights (Article 10), the European Union Charter of Fundamental Rights (Article 11), the American Convention on Human Rights (Article 13), the African Charter on Human and People's Rights (Article 9) and the ASEAN Human Rights Declaration (Article 23).
11. See e.g., the UN Human Rights Committee, General Comment No. 34, adopted on July 2011.
12. Joint Declaration on Freedom of Expression and the Internet, UN Special Rapporteur on Freedom of Opinion and Expression (Special Rapportuer on FOE), the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, 1 June 2011; HRC Internet resolution, op.cit..
13. See, e.g. UN Administrative Committee on Coordination, Statement of the Administrative Committee on Coordination on universal access to basic communication and information services, ACC/1997/4, 25 June 1997; UN General Assembly, UN Millennium Declaration, Resolution adopted by the GA, 18 September 2000, A/RES/55/2; UN and ITU, Declaration of Principles: a global challenge in the new Millennium, World Summit on the Information Society, WSIS-03/GENEVA/DOC/4-E, 12 December 2003; the May 2011 Report of the Special Rapporteur on FOE: Addendum, Communications to and from Governments, op.cit., para 60; UN GA, Report of the Special Rapporteur on FOE, 10 August 2011, A/A/66/290, paras 61 and 63; OECD, OECD Council Recommendation on Principles for Internet Policy Making, 13 December 2011, Principle 2; HRC Internet resolution, op.cit.; UN GA, Transforming our world: the 2030 Agenda for Sustainable Development, 21 October 2015, A/RES/70/1, Goal 9.c; the webpage of Internet Governance Forum; Internet Rights and Principles Dynamic Coalition, UN Internet Governance Forum, The charter of human rights and principles for the internet, August 2014, 4th Edition; or Council of Europe, Committee of Ministers, Recommendation No.R (99) 14 on universal community service concerning new communication and information services, 9 September 1999. At the national level, a number of European countries have recognised the right to access the Internet within their legal frameworks either through constitutions, laws or court's rulings; see, e.g. Republic of Estonia, Public Information Act, 15.11.2000, article 33 and the Constitution of the Republic of Estonia, 29 June 1992, article 44; The Constitution of Greece, as revised by the parliamentary resolution of April 6th 2001, article 5A.2, Republic of Finland, Communications Market Act, 393/2003, amendments 363/2011, Section 60c(2); Kingdom of Spain, Law on Sustainable Economy, 2/2011, 4 March 2011, Article 52.
14. The 2011 Report of the Special Rapporteur on FOE to the UN General Assembly, op.cit., para 87.
15. This test has been restated in numerous international human rights instruments, most notably in the Human Right Committee's General Comment No. 34.
16. 2011 Joint Declaration, op.cit.
17. HRC Internet Resolution, op.cit.
18. General Comment No. 34, op.cit. para 43.
19. See the European Convention on Human Rights (Article 8), the European Union Charter of Fundamental Rights (Article 7) and the American Convention on Human Rights (Article 11).
20. The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981.

21. UN General Assembly Guidelines for the Regulation of Computerized Personal Data Files, as adopted by General Assembly resolution 45/95 of 14 December 1990.
22. G. Greenleaf, Asian Data Privacy Laws (Oxford, Oxford University Press: 2014), 55. For details about each of the domestic frameworks, see BakerHostetler, 2015 International Compendium of Data Privacy Laws.
23. See e.g.: European Court (ECtHR) decisions in *Leander v. Sweden*, App. No. 9248/81, 26 March 1987; *S. and Marper v. the UK*, App. Nos. 30562/04 and 30566/04, 4 December 2008; Malone v. the UK, No. 8691/79, 2 August 1984; Copland v. the UK, No. 62617/00, 3 April 2007; Klass and Others v. Germany, No. 5029/71, 6 September 1978; ECtHR, Uzun v. Germany, No. 35623/05, 2 September 2010; or the decisions of the Court of Justice of EU (CJEU) in C-293/12 and C-594-12, Digital Rights Ireland v Ireland, 8.4.2014; or C-362/14, Schrems v Data Protection Commissioner, 6.10.2015.
24. In 2012, ASEAN adopted a Human Rights Declaration which specifically references the protection of personal data, and in 2014 the African Union adopted a Convention on Cyber Security and Personal Data Protection.
25. In its Concluding Observations of its 2014 review of the USA's compliance with its obligations under Article 17 of the ICCPR, the Committee noted that interferences with the right to privacy must comply "with the principles of legality, necessity and proportionality;" CCPR/C/USA/CO/4, para 22. This sentiment echoed that of the Special Rapporteur on FOE in his 2013 report on privacy and communications surveillance, who stated that "[t]he framework of article 17 of the ICCPR enables necessary, legitimate and proportionate restrictions to the right to privacy by means of permissible limitations", the test of which should be understood to be in the same terms as that applicable under Article 19, paragraph 3, despite Article 17 not containing such explicit language. The UN High Commissioner on Human Rights, in her 2014 report, The right to privacy in the digital age, confirmed the Special Rapporteur's interpretation, stating: "[…] authoritative sources point to the overarching principles of legality, necessity and proportionality…;" A/HRC/27/37, para 23.
26. Reflected in the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (known as Convention 108); and the 1990 UN guidelines for the regulation of computerized personal data files.
27. These Principles are taken from Article 5 of the General Data Protection Regulation but they broadly reflect the US Federal Trade Commission's Fair Information Processing Principles, the Principles enshrined in the OECD's and UN's Guidelines, Convention 108 and the European Data Protection Directive, which has informed data protection regulations in more than one hundred countries around the world.
28. These include General Comment No. 34, op.cit., HRC Internet Resolution op.cit.; the 2011 Joint Declaration op.cit.; Reports of the Special Rapporteur on freedom of expression on the Internet (A/66/290, 2011), surveillance and the right to privacy (A/HRC/23/40, 2013), access to information (A/68/335, 2014), and the protection of sources and whistleblowers (A/70/361, 2015); decisions of the ECtHR in *Delfi AS v. Estonia* [GC], App. No. 64569/09, 16 June 2015; Editorial Board of Pravoye Delo & *Shtekel v. Ukraine*, App. No. 33014/05, 5 May 2011; *Niskasaari & Otavamedia Oy v. Finland*, App. No. 32297/10, paras 9 and 54-59, 23 June 2015; *Mosley v. the UK*, App. No. 48009/08, § 129, 10 May 2011; *Animal Defenders International v. the UK* [GC] App. No. 48876/08, § 119, or *Ahmet Yıldırım v. Turkey,* App. No. 3111/10, § 67, ECHR 2012.
29. Report of the Special Rapporteur on FOE on telecommunications and Internet access sector, A/HRC/35/22, 30 March 2017. The Special Rapporteur's May 2016 report to the General Assembly (A/HRC/32/28) is also instructive
30. *Op.cit.*
31. The United Nations Global Compact is a UN initiative to encourage businesses worldwide to adopt sustainable and socially responsible policies, and to report on their implementation,
32. The Guiding Principles were launched in 2008 under the leadership of UN Special Representative John Ruggie. They built upon the work of the UN Global Compact, launched in 2000 to encourage business to develop responsible business practices
33. Telecommunications Industry Dialogue Guiding Principles, 12 March 2013.
34. Global Network Initiative, Global Principles on Freedom of Expression and Privacy, developed by companies, investors, civil society organizations and academics
35. Ranking Digital Rights, Corporate Accountability Index.
36. Ranking Digital Rights, 2015 Corporate Accountability Index Indicators.
37. CDT, Iran's Internet Throttling: Unacceptable Now, Unacceptable Then, 3 July 2013; Software Freedom Law Centre India, Internet Shutdowns in India, 2016; Access Now, Gambia shuts down Internet on eve of elections, 30 November 2016.
38. See CDT, Network Shutdowns Timeline, 11 September 2014.
39. E.g. in India, Algeria, Ethiopia, Iraq and Azerbaijan; see Special Rapporteur on FOE 2017 Report, op.cit.
40. D. O'Brien, Venezuela's Internet Crackdown Escalates into Regional Blackout, EFF, 20 February 2014.
41. See e.g., Preliminary observations by the Special Rapporteur on FOE at the end of his visit to Tajikistan, 9 March 2015;
42. General Comment No. 34, op.cit., para 43.
43. Such laws exist in South Korea, New Zealand, France and the United Kingdom; other countries, like Australia, have considered and abandoned such an approach.
44. The French HADOPI law, adopted in 2009, allowed the suspension of Internet access until the relevant provisions were found unlawful in 2013. There was a also voluntary "six strikes" programme in the USA (so called the Copyright Alert System) which functioned to the same effect; the programme was retired in January 2017.
45. UN Special Rapporteur on FOE, Report to the HRC, June 2011 (A/HRC/17/27), para 78.
46. A. Futter & A. Gillwald, Zero-rated Internet services: What is to be done?, Research ICT Africa.
47. J. Malcolm, C. McSherry & K.Walsh, Zero Rating: What It Is and Why You Should Care, 18 February 2016.
48. In Morocco, Skype, Viber, Tango, WhatsApp, and Facebook Messenger are among the applications whose VoIP calls have been blocked by telecom operators on 3G and 4G connections in January 2016 and ADSL connections in February 2016. In China, any VoIP services that are not offered by state telcos are prohibited.
49. In Brazil, Whatsapp was temporarily blocked in 2016; see ARTICLE 19, Brazil: WhatsApp services blocked nationwide in violation of freedom of expression, 22 July 2016.
50. In 2016, the United Arab Emirates President issued a number of special federal laws relating to Internet crimes, including a regulation that forbids anyone in the UAE from making use of virtual private networks (VPN).

51. Content agnosticism refers to the notion that network traffic is treated identically regardless of payload, with some exception where it comes to effective traffic handling, for instance where it comes to delay tolerant or delay sensitive packets, based on the header. Content agnosticism prevents payload-based discrimination against packets; see N. ten Oever, Human Rights Protocol Considerations Research Group, Research into Human Rights Protocol Considerations draft-irtf-hrpc-research-11.
52. See, e.g. ARTICLE 19, Our 5G future: Light at the end of the tunnel or Internet fast-lane for the elite?, 15 September 2016.
53. 5G Manifesto for timely deployment of 5G in Europe, 7 July 2016.
54. See, e.g., The Register, EU operators' 5G manifesto misses the point, 13 July 2016;
55. Such as Chile, Norway, the Netherlands, Finland, Iceland, Estonia, Latvia, Lithuania, Malta, and Japan.
56. See, e.g. FCC, Protecting and Promoting the Open Internet, FCC 15-24, 12 March 2015
57. See European Commission, Our Commitment to Net Neutrality, October 2015.
58. In 2016, the UK enacted the Investigatory Powers Act 2016, which requires telecommunications providers to generate and retain "Internet connection records" for up to 12 months
59. Australia is the country to have adopted such a law. In 2014, the European Data Retention Directive was invalidated, rolling back data retention laws across Europe, although subsequent data retention regimes have been enacted. In the USA, data retention is mandated by the USA Freedom Act since 2015; prior to that, Section 215 of the Patriot Act imposed similar requirements.
60. Inter-American Court of Human Rights, *Escher et. al. v. Brazil*, 6 July 2009, para 114.
61. See, CJEU, *Watson and others v UK* 698/15 (Joined Cases C-203/15, C-698/15), 21 December 2016, paras 99-101.
62. UN High Commissioner for Human Rights Navi Pilla, *The right to privacy in the digital age,* para 27.
63. CJEU, *Watson and others v UK, op.cit.*, paras 105-106.
64. ECtHR, *Zakarov v Russia*, App. No. 47143/06, 4 December 2015, para [229].
65. ECtHR, *Weber and Saravia v Germany,* App. No. 54934/00, para. [95]
66. See, e.g., the HR Committee's Concluding Observations to the USA (CCPR/C/USA/CO/4), 2014, para 22.
67. ECtHR, *Zakarov v Russia, op.cit.* para [260].
68. Access Now, Forgotten Pillar: The Telco Remedy Plan, May 2013.
69. Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users, Council of Europe.
70. European Commission ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights, 2013.
71. The Guiding Principles, op.cit., Principle 23 – Issues of Context
72. Much of this guidance is taken from the European Commission ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights, p. 53.
73. C.f. the 2017 report of the Special Rapporteur on FOE, op.cit.

**DEFENDING FREEDOM OF EXPRESSION AND INFORMATION**

ARTICLE 19 Free Word Centre 60 Farringdon Road London EC1R 3GA
**T +44 20 7324 2500 F +44 20 7490 0566**
**E info@article19.org W www.article19.org Tw @article19org facebook.com/article19org**