ARTICLE 19

The Global Principles on Protection of Freedom of Expression and Privacy

Policy Brief

Table of contents

Introduction

Freedom of expression and privacy are mutually reinforcing rights – all the more so in the digital age. Both are essential foundations for open and democratic societies, and among the basic conditions for its progress, and for each individual's self-fulfilment. For democracy, accountability and good governance to thrive, freedom of expression and opinion must be respected and protected. The same is true of the right to privacy, which also acts as a powerful bulwark against state and corporate power in the modern age.

While freedom of expression is fundamental to diverse cultural expression, creativity and innovation as well as the development of one's personality through self-expression, the right to privacy is essential to ensuring individuals' autonomy, facilitating the development of their sense of self and enabling them to forge relationships with others.

Privacy is also a pre-requisite to the meaningful exercise of freedom of expression, particularly online. Without privacy, individuals lack the space to think and speak without intrusion and to develop their own voice. Without freedom of expression, individuals would be unable to develop their sense of self. At the heart of the protection of these rights lies the respect for, and protection of, human dignity and individuals' ability to live freely and engage with one another.

At the same time, one person's right to freedom of expression may impinge on someone else's right to privacy and vice versa. This tension is exacerbated by digital technologies. Whilst they have been central to the facilitation of the exercise of freedom of expression and the sharing of information, digital technologies have also greatly increased the opportunity for violations of the right to privacy on a scale not previously imaginable. In particular, digital technologies present serious challenges to the enforcement of the right to privacy and related rights because personal information can be collected and made available across borders on an unprecedented scale and at minimal cost for both companies and states. At the same time, the application of data protection laws and other measures to protect the right to privacy can have a disproportionate impact on the legitimate exercise of freedom of expression.

These Principles were developed in order to provide a systematic analytical framework for assessing the ways in which the rights to freedom of expression and privacy are mutually reinforcing, and for determining the permissible limits which can be placed on these rights where they are in conflict, both on and offline. In particular, the Principles seek to ensure that both of these fundamental rights are effectively respected and protected in the digital age. As we demonstrate in these Principles, international law provides a framework to resolve tensions and maximise the enjoyment of both rights. The Principles we set out here offer a progressive interpretation of international law and best practice in individual states, as reflected, *inter alia*, in national laws and the judgments of national courts. They should be interpreted in the most favourable way for human rights.

These Principles should neither be taken as foreclosing nor as approving restrictions designed to protect other interests – including the protection of reputation by defamation laws – which deserve separate treatment and are addressed in their entirety in a separate set of principles.

It is our intention and hope that these Principles will be used by individuals, activists, campaigners, legal practitioners, intermediaries, judges, elected representatives, parliamentarians, and public

officials around the world as they seek to respect, protect, and fulfil the rights to freedom of expression and privacy.

Preamble

We – individuals and organisations – who endorse and agree to these Principles

Affirming that the rights to freedom of expression and to privacy are among the essential foundations of an open and democratic society, and among the basic conditions for its progress and for the enjoyment of other human rights and fundamental freedoms;

Considering that the protection of the right to privacy is a necessary pre-condition for the meaningful exercise of the right to freedom of expression and human development;

Noting that individuals are much more likely to express controversial viewpoints or share sensitive information in the knowledge that their anonymity and the privacy and security of their communications are protected, including through the use of anonymity, encryption, and other security tools;

Fully aware that the right to freedom of expression is also a necessary component of the development of individuals' personality and identity;

Considering that the rights to freedom of expression and privacy are therefore often mutually reinforcing rights;

Taking note, however, that the right to freedom of expression and the right to privacy may in certain circumstances come into conflict, including where privacy claims may be used without justification to prevent the dissemination of information about individuals in order to restrict reporting on matters of public interest and to avoid public scrutiny, or deliberately mislead others;

Recognising at the same time that the dissemination of private information without justification may seriously infringe the right to privacy, particularly that of persons in situations of vulnerability;

Desiring to promote a clear framework for the protection and promotion of both the rights to freedom of expression and privacy where they are in conflict, especially online;

Taking into account the relevant provisions of the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the African Charter on Human and Peoples' Rights, the American Convention on Human Rights, the European Convention on Human Rights and the EU Charter of Fundamental Rights and Freedoms;

Having regard to the UN Guiding Principles on Business and Human Rights (Ruggie Principles), the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the International Principles on the Application of Human Rights to Communications Surveillance (The Necessary and Proportionate Principles), the Johannesburg Principles on National Security, Freedom of Expression and Access to Information, the Global Principles on National Security and the Right to Information (Tshwane Principles), the Revised Defining Defamation: Principles on the Freedom of Expression and the Protection of Reputation, the Manila Principles on Intermediary Liability and the Joint Declaration on Freedom of Expression and the Internet of the UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special

Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of Expression and Access to Information on 1 June 2011;

Noting that nothing in these Principles should be interpreted as setting a lower threshold for the protection of the rights to freedom of expression and privacy than that provided by relevant international and regional instruments;

Bearing in mind that the dissemination of, and access to, information is a basic requirement to foster accountability and a society free of corruption, to promote access to knowledge, development and culture, which is the common heritage of all humankind, and which should be cherished, upheld, and made accessible for the benefit of all;

Recognising that the Internet is a global resource which should be managed in the public interest and that digital technologies have greatly enhanced freedom of expression and access to information whilst, at the same time, posing great challenges to the protection of individuals' right to privacy and to the protection of personal data;

Concerned about the serious risks big data poses to the right to privacy and to the protection of personal data, while noting the potential benefits of opening large data sets for society as a whole;

Considering that data protection is essential to ensure that individuals are involved in decisions concerning their personal data and to ensure that states and companies that gather and record personal data are transparent about the data they hold; follow fair and lawful processes on the collection, use, retention and maintenance of security of that data; and ensure that personal data collected for one purpose is not used for another;

Aware that data protection legislation can be misused or abused to prevent, end or restrict the legitimate public dissemination of accurate personal information in order to enable individuals to control their reputation at the expense of freedom of information, the right to truth and the wider public interest;

Call on all appropriate bodies at international, regional, national and local levels and on private actors, to endorse, promote, respect, and apply these Principles in their policies and practices. We also recommend that they give effect to these Principles and engage in their dissemination, acceptance, and implementation at all levels.

Definitions of key terms

For the purposes of these Principles,

a) The term *confidential information* means any information to which a "duty of confidence" applies. A duty of confidence is created when:

i. Private information has been passed or disclosed in such a way that the person receiving the information knew, or ought to have known, that the information was being imparted on the basis of confidentiality; or

ii. When private information has been disclosed in circumstances where it is reasonable to expect that the information will be held in confidence.

Confidential information must not be used or disclosed without the explicit consent of the individual concerned, absent a specific legal basis, or absent a robust public interest or legal justification to do so;

b) The term *data controller* means the natural or legal person which, alone or jointly with other persons, determines the purposes for which, and the manner in which, any personal data are, or are to be, processed;

c) The term *data protection rights* refers to the range of rights that individuals (data subjects) possess under data protection law. Data protect rights include but are not limited to the:

i. Right to ensure that data is stored and processed lawfully (on the basis of consent or some other lawful basis laid down by law), fairly and securely;

ii. Right to know what personal data is held about them by controllers (right of access) and for what purpose;

iii. Right to seek to correct that data when it is inaccurate (right of rectification);

iv. Right to demand that data be deleted when it is no longer necessary for the permitted purpose, when it is irrelevant or out-of-date, when consent has been withdrawn and there is no other lawful basis, when the data has been unlawfully processed, or when it has been made public without justification (right to erasure);

v. Right to receive one's personal data from a data controller for the purpose of changing a service (data portability); and

vi. Right to object to the processing of data for particular purposes, including for direct marketing and profiling, where certain conditions apply (right to object).

d) The term *informed consent* in the context of data protection means an individual's freely given agreement (not obtained under duress, coercion, or by fraud), based on adequate knowledge and understanding of information relevant to the processing of his/her personal data. The individual giving consent must be informed about the purpose of the data collection, processing or use of the data, and the consequences of a refusal to give consent if necessary or if the individual so requests. The consent must be referenced to a clearly determined processing; to the extent sensitive personal data are concerned the consent obtained must refer explicitly to such sensitive personal data;

e) The term *journalism* refers to the function of regularly or professionally engaging in the collection and dissemination of information to the public via any means of mass communication. It involves but is not limited to the collection (research, interviews or freedom of information requests) and production (including writing, data analysis, and verifying material) of information. It can also include editorial, publication or broadcast activities, and management of standards (including staff training, management, and supervision);

f) The term *personal data* means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, or social identity;

g) The term *principle of maximum disclosure* refers to a presumption that all information held by public bodies should be subject to disclosure and that this presumption may be overcome only in very limited circumstances;

h) The term *public interest* encompasses matters in which the public has an interest or concern of being informed. This includes, but is by no means limited to, information about matters that affect the functioning of the state, public officials and public figures, politics, public health and safety, law enforcement and the administration of justice, the protection of human rights, consumer and social interests, the environment, economic issues, the exercise of power, art and culture, or matters that affect general interests or entail major consequences;

i) The term *public figure* means an individual engaged in public life. It includes leaders of states and elected representatives, public officials, business leaders, people in the public eye who have a platform as a result (including "celebrities") or individuals engaged in a public interest activity or performing a public function;

j) The term *public authority* means any natural or legal person exercising administrative authority, or holding public responsibilities or functions, or providing public services, or operating with substantial public funds for public matters;

k) The term *request to be de-listed* means a remedy that enables individuals to request to be de-listed from search results produced on the basis of a search term which includes their name. This remedy has been derived from the "right to erasure" under data protection law by some international and domestic courts and is sometimes inaccurately referred to as "the right to be forgotten";

l) The term *right to truth* means the right to seek, receive and impart information about human rights violations. It is a collective right drawing upon history, recent or current events to prevent violations from recurring in the future. Its corollary is a "duty to remember", which the state must assume, in order to guard against the perversions of history that go under the names of revisionism or negationism. States have a corresponding obligation to facilitate the uncovering of information about human rights violations, whether past or present, particularly where violations have occurred on a large, systematic scale and entire societies need to come to terms with the events which occurred;

m) The term *sensitive personal data* means personal data consisting of information relating to the data subject with regard to racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; trade union membership and membership in other associations; physical or mental health or condition; sexual life, sexual orientation, gender identity or expression; genetic data; biometric data for the purpose of uniquely identifying a natural person; the commission or alleged commission by the data subject of any offence; or any proceedings for any offence committed, or alleged to have been committed, by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings;

n) The term *search engines* refers to software programs that use sophisticated algorithms to retrieve data, files or documents from a database or network in response to a query. The information retrieved is usually indexed and presented as a series of hyperlinks on a webpage;

o) The term *social media platforms* refers to platforms the distinctive feature of which is that they encourage individuals to connect and interact with other users and to share content;

p) The term *substantial harm* means actual, or substantial risk of, physical harm, severe mental distress or anguish, loss of, or detriment to, employment. Mere embarrassment or discomfort and potential loss of business or job prospects are not sufficient to qualify as substantial harm;

q) The term *web hosting providers or hosts* refers to bodies (typically companies) that rent web server space to enable their customers to set up their own websites;

r) The term *persons in situations of vulnerability* is used to describe persons whose particular social location in society more broadly and within the community renders them at a particularly high risk of physical or emotional harm. Persons in situations of vulnerability include, but are not limited to, children, elderly, persons with disabilities, the recently bereaved, the seriously ill or persons who face discrimination based on their gender, or sexual orientation or gender identity.

Section 1: General principles

Principle 1: Legal framework for the protection of rights

States should ensure that the right to freedom of opinion and expression, the right to information and the right to privacy are enshrined in domestic constitutional provisions or their equivalent, in accordance with international human rights law. Domestic legislation should include that everyone has:

a) *The right to freedom of expression,* which includes the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media or other platforms of his or her choice. The right to freedom of expression includes the right to offend, criticise, comment or talk about others, including on aspects of their private life, which are either private or known to the public, without their consent;

b) *The right to hold an opinion* without interference or limitations as defined under Principle 2;

c) *The right to information,* which includes the right of everyone to seek, receive, use, and impart information held by or on behalf of public authorities, or to which public authorities are entitled by law to have access, and information held by private bodies exercising public functions and required for the exercise or protection of any right or fundamental freedom;

d) *The right to privacy,* which includes the right of individuals to respect for their private and family life, home, and communications and the right to the protection of the law against arbitrary or unlawful interference or attacks against them. The *right to private life* extends to aspects relating to personal identity, such as a person's name, images, or physical and moral integrity; it is primarily intended to ensure the development, without outside interference, of the personality of each individual in his/her relations with other human beings;[1]

e) *The right to personal data protection,* which may be derived from, and be related to, the right to privacy; and which regulates the way in which information about individuals, which may be either private or public, is collected, processed, stored and retained electronically by both public and private bodies. Personal data must be processed lawfully and fairly for specified purposes and on the basis of the informed consent of the person concerned, or some other legitimate basis laid down by law. Without prejudice to the applicability of data protection rights under this Principle, personal information may be processed without the consent of the individual if the information is publicly available. Everyone should have the right of access to data held by third parties (data controllers) concerning him or her, and the right to have it rectified or deleted, subject to legitimate exceptions.

[1] This provision should not be used to prevent states providing full protection of rights as provided for by Article 18 of the International Covenant on Civil and Political Rights.

Principle 2: Limited scope of permissible restrictions

2.1. States should ensure that domestic constitutional or legal provisions clearly set out the scope of permissible restrictions on the rights and freedoms set forth in these Principles. States should provide that such restrictions may only be justified if they are:

a) *Provided by law*: any restriction must have a formal basis in law, which is accessible and formulated with sufficient precision to enable individuals to foresee whether a particular action is in breach of the law and to assess the likely consequences of any breach;

b) *In pursuit of a legitimate aim*: any restriction must be shown by the state to have the genuine purpose and demonstrable effect of protecting a legitimate aim recognised under international law, which includes the rights and freedom of others;

c) *Necessary and proportionate in pursuance of a legitimate aim:* any restriction is necessary and proportionate in a democratic society if it is the least restrictive means available for protecting that interest; and

d) Restrictions on the right to hold an opinion (as provided for in Principle 1b) are never permitted.

2.2. States should ensure that domestic legislation provides for sufficient safeguards and remedies against abuse, including prompt, full and effective scrutiny, by an independent court, tribunal or other independent adjudicatory body of the validity of the restriction.

2.3. States must not merely abstain from interfering with the rights and freedoms set forth in these Principles, they also have positive obligations to protect them, including from interference by third parties.

2.4. Private actors should respect the rights and freedoms set forth in these Principles, including the limited scope of permissible restrictions on them as provided herein.

Principle 3: Legitimate purpose of privacy causes of action

States should recognise and give effect to the following:

a) Laws providing for privacy offences and/or torts may constitute legitimate restrictions on the right to freedom of expression if they are sufficiently clear and narrowly defined and their genuine purpose and demonstrable effect is to protect individuals from unlawful interferences in, or attacks on, their right to private and family life, home and communications;

b) Laws protecting individuals from substantial harm, including but not limited to harassment, threats of violence, the malicious disclosure or distribution of private sexual content (including photographs or films), or malicious disclosure of sensitive personal information or personal information other than a person's name or other identifier without consent can constitute a legitimate restriction on the right to freedom of expression provided that they are narrowly drawn, contain sufficient defences for the protection of freedom of expression and do not impose disproportionate sanctions;

c) Laws providing for privacy offences and/or torts cannot be justified if their purpose is merely to protect individuals against harm to a reputation which they either do not have or do not merit. In particular, privacy offences or torts cannot be justified if their purpose or effect is to prevent legitimate criticism of public figures, the exposure of corruption, official wrongdoing, or to protect the reputation of heads of state or other public officials or public figures;

d) Laws providing for privacy offences or torts cannot be justified on the grounds that they help maintain public order, national security, or friendly relations with foreign states or governments.

Section 2: Freedom of expression and the right to privacy as mutually reinforcing rights

Principle 4: Communications surveillance

4.1. The indiscriminate and untargeted collection, storage and analysis of digital and traditional communications or communications data without specific, individual reasonable suspicion ("mass surveillance") by state and non-state actors impinges on the very essence of the right to privacy. It also has a chilling effect on the exercise of the right to freedom of expression and the right to hold and form an opinion by searching and accessing and disseminating information online. As such, mass surveillance is always a disproportionate interference with the rights to privacy and freedom of expression.

4.2. States should ensure that their legislation, practices, and procedures regarding the surveillance of communications comply with the International Principles on the Application of Human Rights to Online Communications Surveillance.

Principle 5: Mandatory data retention

Mandatory retention laws – requiring Internet and telecommunications service providers to continuously collect and preserve the content of users' communications, communications data as well as information about users' online activities and identity – significantly interfere with the rights to freedom of expression and privacy. States should ensure that their data retention regimes and schemes fully comply with standards set forth in these Principles taking into consideration the following:

a) General and indiscriminate mandatory retention measures are a disproportionate restriction on the rights to privacy and freedom of expression and should be abolished; and

b) Targeted retention measures should only be imposed where they are necessary for the purpose of fighting serious crime, where the categories of data to be retained and the retention period is limited to what is strictly necessary, and where they are accompanied by safeguards against abuse.

Principle 6: Anonymity, mandatory user registration and real-name requirements

6.1. Everyone should have a right to exercise his/her right to freedom of expression anonymously, which includes through anonymous speech, to read anonymously or to access information in online and physical environments anonymously.

6.2. There should be a presumption in favour of exercising this right. States should repeal:

a) Blanket prohibitions on anonymity as these are unnecessary and disproportionate restrictions on the rights to privacy and freedom of expression;

b) Laws, regulations and policies requiring the registration of real names or other identifiable information or imposing the registration of devices and connections as a pre-

requisite for access to the Internet or Internet services, as these constitute a violation of the rights to freedom of expression and privacy.

6.3. Service providers should ensure that their users can communicate anonymously, and thus refrain from imposing real-name policies or requiring the registration of other identifiable information on their platforms, as such requirements severely undermine the rights to freedom of expression and privacy.

Principle 7: Encryption

7.1. Everyone should have a right to use secure communication tools, in particular any hardware and software encryption products and other cryptographic methods of their choice.

7.2. States should recognise in their legislation and practices that encryption is a basic requirement for the protection of the confidentiality and integrity of information and that, as such, it is essential to the protection of the rights to privacy and freedom of expression online.

7.3. States and companies should promote end-to-end encryption of communications as the basic standard for the protection of the right to privacy online. They should also promote privacy by design in technical standards and company products.

7.4. States should promote digital literacy (the set of enabling skills that are required to use digital technology) in the use of encryption tools and promote the use of open source software, including by ensuring that it is regularly and independently maintained and audited for vulnerabilities, including by civil society experts.

7.5. States should refrain from adopting or repeal all legislation that prohibits individuals from using encryption or prohibits companies from including encryption in their systems and products.

7.6. States should refrain from adopting measures requiring or promoting technical vulnerabilities ("backdoors") to be installed in hardware and/or software encryption products as a disproportionate restriction on the right to privacy and a disproportionate form of compelled expression.

7.7. States should repeal or refrain from adopting laws requiring the disclosure of decryption keys. Court-ordered decryption of encrypted data or devices (as opposed to disclosure of decryption keys) may only be permissible when it results from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals responsible for the encryption and only when subject to judicial warrant and respect for due process rights of individuals, including the right against self-incrimination.

7.8. States should refrain from adopting laws establishing key escrow systems.

7.9. States should lift import/export restrictions on encryption hardware and software.

Principle 8: Data disclosure by companies

8.1. Service providers should only be required to disclose personal information about their users subject to a court order, which must be in line with the requirements of legality, legitimate aim, necessity, and proportionality under international human rights law.

8.2. Service providers should notify their users that access to their personal data has been sought by state authorities or third parties except in cases where non-disclosure has been specifically ordered by a court for a limited period of time because disclosure would create a real risk of harm to another individual or would allow individual suspects to destroy evidence and seriously jeopardise an investigation.

8.3. Service providers should publish transparency reports with specific information about all requests and/or orders for disclosure of personal data they receive from states, courts, and private parties. This should also include information about actions taken by the company on such requests or orders.

8.4. Consistent with Principle 8.3, states should repeal laws, regulations and policies prohibiting service providers from publishing transparency reports on data requests or communications surveillance.

Principle 9: Protection of sources

9.1. The right to freedom of expression implies that everyone who obtains information from confidential sources with a view to exercising a journalistic activity has, subject to Principles 9.2 a) and b), a duty not to disclose the identity of their confidential sources and a right not to be required to do so.

9.2. States should provide for the protection of the confidentiality of sources in their legislation and ensure that:

a) Any restriction on the right to protection of sources complies with the three-part test under international human rights law, as set out in Principle 2;

b) The confidentiality of sources should only be lifted in exceptional circumstances and only by a court order, which complies with the requirements of a legitimate aim, necessity, and proportionality. The same protections should apply to access to journalistic material;

c) The right not to disclose the identity of sources and the protection of journalistic material requires that the privacy and security of the communications of anyone engaged in journalistic activity, including access to their communications data and metadata, must be protected. Circumventions, such as secret surveillance or analysis of communications data not authorised by judicial authorities according to clear and narrow legal rules, must not be used to undermine source confidentiality; and

d) Any court order under 9.2 b) and c) must only be granted after a fair hearing where sufficient notice has been given to the journalist in question, except in genuine emergencies.

Principle 10: Search and seizure

Access to, and search and seizure of, information represents a significant interference with the right to privacy and freedom of expression. States should take immediate steps to ensure that measures regulating access to, search and seizure of, information fully comply with the following conditions:

a) Access to, and search and seizure of information is only justified if the measures strictly comply with the requirements of legality, legitimate aim, necessity, and proportionality;

b) Search of individuals' home or workplace, online accounts, remote data storage, collection of metadata and any seizure of information may only be compatible with the rights to freedom of expression and privacy if ordered by a court and if strictly compliant with the requirements of legality, legitimate aim, necessity, and proportionality under international human rights law;

c) In determining whether the search or seizure of information is necessary and proportionate, special weight must be given to the confidentiality of sources, journalistic material, and privileged information in appropriate cases; and

d) General search and seizure warrants, which are not narrowly drawn and based on reasonable suspicion are inherently disproportionate.

Principle 11: Trans-border data flows

11.1. The meaningful exercise of the right to freedom of expression requires that the right to privacy and personal data protection be strongly protected, including in legal agreements for data flows. In order to ensure a consistent level of protection of personal data, the data protection principles set forth in Section 1 and Section 2 must also apply to data transfers between companies and states.

11.2. In data transfer agreements, states should ensure that the applicable law is the one providing the highest protection for personal data. The level of data protection applicable to an individual's personal data must not be lowered because of the data being transferred.

11.3. All states should adopt data protection laws. Any data localisation laws should ensure strong privacy protections and include limits on access and data retention as set out in Principles 5 and 8.

Section 3: Reconciling the right to freedom of expression and the right to privacy

Principle 12: Publication of personal information

National legal systems should make it clear, either explicitly or through authoritative interpretation, that in the context of the publication of personal information in the news media (including print press and broadcasting) and other platforms:

a) When seeking to reconcile the right to freedom of expression and the right to privacy, particularly in cases involving the publication of personal information, public authorities, the courts or other independent adjudicatory bodies should give regard to all the circumstances of the case, including the following factors:

i. The extent to which the publication at issue contributes to a debate of public interest as defined in the Key Definitions;

ii. The degree of notoriety or vulnerability of the person affected;

iii. The subject covered by the publication and the extent of the private nature of the information at issue;

iv. The prior conduct of the person concerned;

v. Content, form, and consequences of the publication, including the sarcastic, humorous or satirical tone used by the author of the publication and the extent to which the harm suffered as a result of the publication of private information has interfered with his or her private life so as to undermine his or her personal integrity;

vi. The way in which the information was obtained and whether this is consistent with Principles 12 b) and 12 c);

vii. The intent of the individual or entity disseminating the information at issue, and in particular whether it was malicious; and

viii. The extent to which the individual whose privacy is at issue is a public figure, as per Principle 13.

b) Where the published material includes photographs, video footage or sound recordings, regard should be had to the circumstances in which the materials were obtained, including, *inter alia*:

i. Whether the individual concerned voluntarily took, or consented to the taking, use or dissemination of the photograph, video footage or sound recording;

ii. Whether the individual consented to the use, disclosure or dissemination of the material;

iii. Whether the material was obtained without the individual's knowledge or was obtained by subterfuge or other illicit means;

iv. The nature and seriousness of the intrusion bearing in mind that images and sound recordings are particularly sensitive personal information, as they reveal a person's unique characteristics; and

v. Any measures taken to minimise the intrusion into the individual's privacy.

c) The use of privacy-invasive investigating techniques, such as hidden cameras, drones, "hacking", undercover reporting or subterfuge, for the purposes of journalism, should only be permitted in circumstances where:

i. There is an overriding public interest in the dissemination of the information sought or discovered;

ii. Such information could not be obtained by any other less privacy-intrusive means; and

iii. Efforts have been made to address privacy concerns by, *inter alia*, blurring the face of the individual/s concerned, editing out information of a private nature or otherwise minimising the intrusion into the individual/s' privacy.

Principle 13: Public figures

13.1. National legal systems should make it clear, either explicitly or through authoritative interpretation, that open and free debate on matters of public interest is at the very core of a democratic society. Public figures, especially heads of state, elected representatives, individuals with a role in public life, exercising a public function or otherwise engaged in public activities, inevitably and knowingly lay themselves open to close scrutiny by both journalists and the public. They therefore have a lower expectation of privacy than ordinary individuals or lesser public officials in relation to matters of public interest.

13.2. The public interest may extend to aspects of their private life as it relates to, or affects, their public role but does not include purely private matters in which the interest of members of the public is, if any, merely salacious or sensational.

13.3 A person ("celebrity") who does not carry out a public function may still be considered to be a public figure for the purposes of Principle 13, if they are a public figure by virtue of their notoriety; or if they draw benefit from being in the public eye and are able to disseminate their views through the media as a result of their being in the public eye.

13.4. The more significant a public figure is, especially in relation to their being an elected representative or to exercising any public function, the more they should be subject to, and tolerant of, the highest levels of scrutiny in accordance with the principles of democratic pluralism.

Principle 14: Open justice

14.1. States should guarantee in their national legislation, and protect and promote in their practices, the principle of open justice or publicity of all judicial actions. This principle demands that the public have a right to know the identity of the parties involved in court proceedings, including suspects in criminal investigations, defendants and witnesses in criminal proceedings, and private parties in civil proceedings; it also implies that court hearings must be held in public and that filming, recording, broadcasting, using social media, and the taking of photographs should be permitted during court proceedings.

14.2. Restrictions on Principle 14.1, including anonymity orders, hearings held in private and bans on the filming, broadcasting, the use of social media or taking of photographs in certain types of proceedings, should only be permitted by an independent court and can only be justified in exceptional circumstances, including:

a) Where the need to protect victims, witnesses, defendants or their close family members from a real and substantial risk of physical violence or other tangible harm clearly outweighs the free expression rights of individuals to report on court proceedings;

b) Where the need to protect the welfare of children or other persons in situations of vulnerability, including their right to privacy, outweighs the public interest in open justice;

c) Where identifying one of the parties would inevitably lead to the unjustified or disproportionate disclosure of confidential information;

d) Where publicity would defeat the object of the hearing, bearing in mind that the sensibilities of the parties involved are no basis for exclusion of the public from judicial proceedings;

e) Where the subject matter of the case involves discussion of justifiably confidential information of one of the parties and a public hearing would undermine that confidentiality; and

f) Where this is required by the interests of justice, for example to prevent prejudice to judicial proceedings.

14.3. Video recording of court proceedings should comply with data protection principles and should take place so as not to disturb the hearing.

14.4. The fact that the public may misinterpret or act inappropriately as a result of court reporting, however accurate, cannot justify a ban on publication of such reports by the press or the public at large.

14.5 In circumstances where some degree of confidentiality is required, it is preferable – where possible – to achieve this through contestable orders ("reporting restrictions") made on notice to the media, rather than by holding hearings *in camera*.

Section 4: Reconciling freedom of expression, data protection and privacy

Principle 15: Protection of publicly available information

15.1. Once information becomes publicly available, the presumption is that it must remain accessible in the public domain indefinitely. The presumption in this Principle does not extinguish any claim for breach of the right to privacy or the application of data protection principles.

15.2. Notwithstanding Principle 15.1, access to publicly available information may be restricted subject to the strict three-part test laid down in Principle 2.

15.3. There should be a presumption that personal information published by an individual about themselves on public platforms, including on social media platforms in which privacy settings have been set to public, may easily become publicly available and that there is therefore a correspondingly low expectation of privacy in respect of such information.

15.4. Companies should have an obligation to make privacy protections clear and easily understandable and ensure that individuals are given adequate control over the information they want to make public and the information they want to keep private or limited to a defined group online. Companies should not change privacy settings unless it is to provide a higher protection of privacy and they should proactively inform their users of any changes to privacy settings.

Principle 16: Requests to delete content authored and originally published by oneself

16.1. There should be a presumption that the right to freedom of expression includes the right not to speak, to change one's opinion and to delete, or to request a hosting provider or third party to delete, content authored and originally published by oneself, including online.

16.2. Principle 16.1 does not apply to content authored by others and hosted or published by third parties about oneself.

16.3. In deciding whether a request for the deletion of content authored and originally published by oneself should be granted by hosts and third parties, regard should be had to the following factors:

a) Whether the request has been made by a child, or a young person;

b) Whether the request has been made by a person in a situation of vulnerability;

c) Whether the request has been made by someone who was a child, a young person or a person in a situation of vulnerability at the time the content in question was authored or published;

d) Whether the content represents that person's own authorship;

e) Whether the person making the request is a public figure or was at the time the content was authored or published;

f) Whether the content at issue is in the public interest; and

g) Whether it is necessary and proportionate to remove the content taking into consideration all the circumstances of the case.

Principle 17: Requests to delete content published by third parties

17.1. Hosts and third parties should not be required to delete or otherwise remove content containing personal information published by third parties on the basis of national data protection laws or the so-called "right to be forgotten".

17.2. Hosts may only be required to delete content containing personal information published by third parties where the publication of the information by a third party constituted an unlawful act, such as it related to privacy offences or offences such as harassment, threats of violence or malicious disclosure or distribution of personal information or private sexual content (such as photographs or films). In determining whether a request for the deletion of content containing private information published by third parties should be granted, regard should be had to Principle 17 and the factors set out in Principles 12 and 13.

17.3. Any deletion or removal of content on any basis must comply with the Manila Principles on Intermediary Liability.

Principle 18: Requests to be de-listed from search results

18.1. To the extent that a so-called "right to be forgotten" is recognised in some jurisdictions, states should ensure that any such "right" is limited to the right of individuals under data protection law to request search engines to delist inaccurate or out-of-date search results produced on the basis of a search for their name.

18.2. As a matter of principle, de-listing requests should be subject to ultimate adjudication by the courts or independent adjudicatory bodies with relevant expertise in freedom of expression and data protection law. As the same time, search engines are more likely to be the first port of call for such requests. Therefore, it is vital that both parties have the right of appeal to an independent and impartial court or adjudicatory body in disputed cases.

18.3. In determining whether or not to grant a de-listing request, the courts or other independent adjudicatory bodies should address themselves to the following non-exhaustive list of factors:

a) Whether the information is personal information;

b) Whether the claimant or plaintiff had a reasonable expectation of privacy with respect to the information, having regard to his or her prior conduct, whether consent had been given, and the prior existence of the information in the public domain;

c) Whether the information is in the public interest, as defined in the Key Definitions;

d) Whether the information at issue pertains to a public figure, as set forth in Principle 13;

e) Whether the information is part of the public record, in particular whether the material at issue has been published or recorded for journalistic, artistic, literary, or academic purposes or has been published by the government in discharge of a legal obligation to make personal data publicly available;

f) In cases where the information at issue is of a public nature or has been made public with the consent of the claimant or plaintiff, whether the claimant or plaintiff has demonstrated substantial harm as a result of the availability of search results linked to their name;

g) How recent the information is and whether it retains public interest value, having regard to the fact that the more recent the information, the more likely it is to be of public interest value, and that certain types of information may retain public interest value indefinitely;

h) Whether alternative remedies, such as seeking voluntary deletion of the content from any third party publisher, a right to reply or a defamation claim would be more appropriate; and whether such remedies should have been exhausted first or instead;

i) Whether granting a request to be de-listed is a proportionate restriction on the right to freedom of expression, having regard to all the circumstances of the case.

18.4. De-listing orders must be limited in scope to the domain name corresponding to the country where the right is recognised and where the individual concerned has established substantial damage.

18.5. Any de-listing of content on the basis of national data protection laws must apply the Manila Principles on Intermediary Liability and include the following procedural safeguards:

a) Data publishers should be notified and have a right to challenge de-listing requests;

b) Data publishers and search engines should have a right of appeal against de-listing orders.

18.6. Consistent with Principles 24 and 25 below, states should refrain from imposing large punitive fines merely for failure to comply with a de-listing request as this is likely to constitute a disproportionate restriction on freedom of expression, due to the inherent chilling effect of such measures.

18.7. Relevant Internet service providers, public bodies and the courts should publish transparency reports about the number and nature of de-listing requests, as well as statistics about the number of requests which are granted or rejected.

18.8 Where de-listing has occurred, in the interests of transparency this should be made clear in the presentation of the search results.

Principle 19: Data protection exemptions

19.1. States should ensure that the enforcement of data protection rights, as defined for the purpose of these Principles, includes broad exemptions or limitations for the exercise of freedom of expression.

19.2. At a minimum, there must be exemptions from the application of, and/or limitations embedded in, data protection laws for the protection of journalistic, literary, academic, and artistic purposes and for the discharge of any legal obligation to make information publicly available, such as the maintenance of archives for historical or other public interest purposes, or under right to information laws; and such exemptions or limitations must be interpreted broadly so as to give meaningful effect to the rights to freedom of expression and to information.

Section 5: Reconciling the right to information, data protection and the right to privacy

Principle 20: General principles on the right to information

20.1. Public bodies, as well as private bodies carrying out public functions, delivering public services, managing public resources or utilising public funds should apply the principle of maximum disclosure when dealing with right to information requests or proactively publishing information about their activities.

20.2. The scope of exceptions to the right to information, including the right to privacy and protection of personal data, must be limited and subject to strict "harm" and "public interest" tests.

20.3. Public bodies must proactively disclose government data, including through the use of accessible formats and anonymised datasets ("open data"), subject to safeguards for the protection of the right to privacy, of the right to personal data protection (as set forth in Principle 1), and of confidential sources (under Principle 9).

Principle 21: Maximum disclosure of personal information about public officials

21.1. States should enable in their legislation and practices that personal information about public officials can and should be disclosed if it:

a) Relates to those individuals' official capacities or is required for the exercise or protection of any right or fundamental freedom; and

b) Relates to a public official's employment, such as his or her performance, salary, assets, and conflicts of interest.

21.2. Consistent with Principle 13, personal data, which may include private information, about public officials should be disclosed where the information at issue is in the public interest. The public interest (as set forth in the Key Definitions) in disclosing the information must be particularly strong when the information is of a purely private or highly sensitive nature.

Principle 22: Official records

22.1. State authorities may hold personal information about private citizens in court records, social programme records, public registers, professional records, archives, public subsidies for business purposes, and records of beneficial ownership in companies. In determining whether to make those records public or (partially) anonymised, governments should have regard to:

a) The free flow of information;

b) Transparency and accountability;

c) Other aspects of the public interest, such as open justice and anti-corruption;

d) Natural persons' rights to privacy;

e) Legal persons' legitimate rights to, and interests in, confidentiality;

f) Accountability for fair handling of information;

g) Public safety and security; and

h) Discrimination against minorities and other persons in situations of vulnerability.

22.2. There should be a presumption that:

a) Court records should be made public where anonymity orders or other reporting restrictions can adequately protect the right to privacy or to a fair trial where the court deems it necessary;

b) Health records, because of their inherently sensitive nature, should not be made public unless there is a strong countervailing public interest in publishing such information in individual cases; and

c) Public records about children, whether medical or pertaining to social programmes, and public records about victims of sexual, institutional, or other types of criminal violence should not be made public other than in an anonymised format.

22.3. In determining whether, under Principle 22.1 or 22.2, it would be fair for personal information held in such records to be made publicly available, the relevant independent authorities should have regard to the following factors:

a) How the information was obtained;

b) The subject's likely expectation regarding disclosure of information;

c) The effect of the disclosure on the data subject, in particular whether he or she would suffer substantial harm as a result of the disclosure;

d) Whether the party expressly refused consent to the disclosure of the information;

e) The content of the information; and

f) The public interest (as defined in Key Definitions) in the information.

22.4. When personal information is made publicly available in data form, including in public databases, there should be no restrictions on the re-use of such data for the purposes of the exercise of freedom of expression, including journalistic, artistic, and literary purposes.

Section 6: Remedies and sanctions

Principle 23: General principles

23.1. States should ensure that redress mechanisms for alleged privacy or data protection violations should be easy to use, quick and effective, and comply with due process standards. Self-regulatory or voluntary redress mechanisms, alternative dispute resolution schemes, such as ombudspersons, and non-pecuniary remedies should be made available and accessible in addition to effective court action.

23.2. Any sanctions imposed by the courts or other independent adjudicatory bodies in order to protect the right to privacy must be proportionate to the harm suffered.

23.3. The courts or other independent adjudicatory bodies should address themselves to the question of whether the remedy being sought is the most appropriate to deal with the breach of privacy or data protection whilst fully respecting the right to freedom of expression.

23.4. The courts or other independent adjudicatory bodies should consider whether non-pecuniary remedies, including an apology, retraction, correction or declaration, or a combination of these, is or are a more proportionate remedy for dealing with privacy or data protection violations than civil or criminal sanctions.

23.5. In cases relating to the Internet, the courts or other independent adjudicatory bodies should consider whether the case has a real and substantial connection with the country in which the court is based and whether the claimant can establish that he or she has suffered substantial harm in that jurisdiction.

Principle 24: Criminal penalties

States should ensure in their domestic legislation and practices that criminal penalties, including imprisonment and punitive fines, are proportionate to the seriousness of the infringement of the right to privacy or data protection, and, if used at all, should be restricted to the most serious cases where there is wilful disregard of the rights of others or gross negligence.

Principle 25: Pecuniary awards

25.1. In assessing the quantum of pecuniary awards for breaches of the right to privacy or data protection, courts should take into account the potential chilling effect on freedom of expression. In particular, they should ensure that pecuniary awards are never disproportionate to the harm suffered and take into account any available non-pecuniary remedies.

25.2. States should ensure in their domestic legislation and practices that the circumstances in which punitive damages may be awarded must be strictly limited to circumstances where there is a wilful disregard (including gross negligence) of the rights or others.

25.3. A fixed ceiling to the quantum of such punitive damages must be applied in privacy or data protection cases where there is non-material harm, and must be related to the ability to pay of the party being punished.

Principle 26: Prior restraint, super injunctions, mandatory pre-moderation and notice prior to publication

States should recognise in legislation and in practice that:

a) As a matter of principle, prior restraint is never compatible with the protection of the right to freedom of expression, even on the grounds of protecting privacy;

b) Interim non-disclosure orders containing a prohibition on reporting the fact of proceedings (i.e. super-injunctions), including the existence of the injunction and any details contained within it, should be considered a disproportionate restriction on the right to freedom of expression;

c) A legal requirement to give notice to an individual whose right to privacy might be engaged prior to publication, so as to enable him or her to seek an injunction is incompatible with the protection of the right to freedom of expression; and

d) A legal requirement to pre-moderate user-generated content constitutes a form of prior-restraint and as such is incompatible with the right to freedom of expression.

Principle 27: Interim injunctions

27.1. Insofar as interim injunctions prohibiting the publication or further publication of private information (i.e. interim non-disclosure orders) may be permitted by law in certain jurisdictions, states should ensure that such injunctions should only be permitted by order of a court in the most exceptional cases where all of the following conditions are met:

a) The applicant can show that he or she would suffer irreparable damage which could not be compensated by subsequent remedies should publication or further publication take place;

b) The court is satisfied that the applicant is likely to establish at a later full hearing (see Principle 27.3 below) that publication or further publication should not be allowed;

c) The court has had particular regard to the impact on freedom of expression, and where the proceedings relate to journalistic, literary or artistic material, the extent to which the material has or is about to become available to the public or the extent to which it is, or would be in the public interest for the material to be published; and

d) The court has had regard to the protection of the rights set out in Principle 1 and has carefully applied the three-part test set out in Principle 2 to the facts of the case.

27.2. Advance notice of an application for an interim non-disclosure order must be given to respondents and any non-parties which have an existing interest in the information sought to be protected by the order. Failure to provide advance notice can only be justified by

compelling reasons, including where there is a real prospect that were a respondent or non-party to be notified they would take steps to defeat the order's purpose.

27.3. Permanent injunctions should never be obtained without a full and fair hearing of the merits of the case. Permanent injunctions should be limited in application to the specific statements found to be in breach of the right to privacy and to the specific people found to have been responsible for the publication of those statements.

Principle 28: Blocking injunctions

States should ensure in their legislation and practice that:

a) Filtering, blocking, removal and other technical or legal limits on access to content – as serious restrictions on freedom of expression – can only be justified if they strictly comply with the three-part test under international law (as set forth in Principle 2); and

b) Wholesale blocking of the Internet or of online services, platforms, or applications for the purposes of protecting the right to privacy are a disproportionate restriction on freedom of expression.

Principle 29: Intermediary liability and content removal

29.1. States should ensure in their legislation and practices that intermediaries which provide services – such as, for example, those providing Internet access, or searching for, or the transmitting, hosting or caching of information – should in principle be immune from both civil and criminal liability for privacy-infringing content disseminated by third parties using those services.

29.2. Intermediaries should not be required to monitor their services actively to prevent privacy infringements.

29.3. Laws governing the liability of intermediaries in respect of privacy-infringing content must contain due process safeguards sufficient to protect freedom of expression and the right to privacy. In principle, intermediaries should only be required to remove privacy-infringing content if the measure is provided by law and ordered by a court, tribunal or other independent adjudicatory body in accordance with the rule of law. Any removal of content should be consistent with the Manila Principles on Intermediary Liability.

29.4. Principle 29.1 and Principle 29.3 are without prejudice to voluntary redress mechanisms that Internet intermediaries should provide for privacy violations under their terms of service in line with the Manila Principles on Intermediary Liability.

Principle 30: Blanket prohibitions on Internet access on grounds of privacy protection

States should refrain from mandating blanket prohibitions on access to the Internet on the grounds of protection of the right to privacy, as these are always a disproportionate restriction on the right to freedom of expression.

Background

These Principles are part of ARTICLE 19's International Standards Series, an ongoing effort to elaborate in greater detail the implications of protecting and promoting the right to freedom of expression in different thematic areas.

These Principles are the result of a process of study, analysis, and drawing on the extensive experience and work of ARTICLE 19's regional offices and partner organisations in many countries around the world. An original draft of the Principles prepared in coordination with the Steering Committee (consisting of Access Now; The Centre for Internet and Society, India; Derechos Digitales; Electronic Frontier Foundation; KICTANet, Kenya; Open Net Korea and Tactical Tech) and further elaborated in a series of consultations, organised by ARTICLE 19, with high-level experts from Africa, Latin America, North America, Europe, and Asia: activists, legal practitioners, academics, and other experts in international human rights law, freedom of expression, privacy, and data protection law. The consultations included one expert meeting in San Francisco on 28–29 March 2016 and a global public consultation launched online in 2016. Broader discussions also took place around the draft that emerged from the meeting and global consultation. The final version of the Principles was produced on the basis of these consultations.

ARTICLE 19 appreciates the input and support of all the individuals and organisations that contributed to the development of these Principles.

These Principles were developed as a part of the project supported by a grant from the Ford Foundation and the Foundation Open Society Institute in cooperation with the Program on Independent Journalism of the Open Society Foundation. The Ford Foundation and The Foundation Open Society Institute do not necessarily share the opinions here within expressed.

ARTICLE 19 bears the sole responsibility for the content of the Principles.