Module 4

Privacy and Security Online

Advanced Modules on Digital Rights and Freedom of Expression Online
ISBN 978-0-9935214-1-6

Published by Media Legal Defence Initiative: www.mediadefence.org

This report was prepared with the assistance of ALT Advisory: https://altadvisory.africa/

This work is licenced under the Creative Commons Attribution-NonCommercial 4.0 International License. This means that you are free to share and adapt this work so long as you give appropriate credit, provide a link to the license, and indicate if changes were made. Any such sharing or adaptation must be for non-commercial purposes and must be made available under the same “share alike” terms. Full licence terms can be found at http://creativecommons.org/licenses/by-ncsa/4.0/legalcode.
Table of Contents

**Scope and the Right to Privacy** ................................................................. 1

**Data Protection** ......................................................................................... 3
  * Key principles for data protection .......................................................... 3
  * Regional data protection frameworks in Africa ..................................... 5
  * Extra-territorial application of data protection frameworks in Europe .... 7
  * Use of data protection authorities to vindicate the right to privacy ........ 10

**Data Retention** ......................................................................................... 11

**Surveillance** ............................................................................................... 13
  * Government-led digital surveillance ....................................................... 13
  * Necessary and proportionate ................................................................. 17
  * Safeguards and oversight ...................................................................... 18
  * Covert recordings .................................................................................. 21

**Collection of Biometric Data and Facial Recognition** ............................ 23

**Encryption and Anonymity on the Internet** ........................................... 26
  * The interplay between encryption and anonymity ............................... 26
  * Encryption ............................................................................................ 27
  * Anonymity ............................................................................................ 31

**Source Protection and the Protection of Journalistic Materials** .......... 35

**Online Harassment** .................................................................................... 38
**MODULE 4**

**Privacy and Security Online**

- To provide an overview of the right to privacy.
- To set out data protection principles.
- To understand data retention.
- To identify issues around the rise in surveillance.
- To understand biometrics and facial recognition.
- To discuss the interplay between encryption and anonymity.
- To understand source protection.
- To identify issues around online harassment.

**Scope and the Right to Privacy**

In the current data-driven era, the right to privacy has gained increasing recognition as a fundamental right, both in itself and as an enabler of other rights. This includes enabling the right to freedom of expression, for instance by allowing individuals to share views anonymously in circumstances where they may fear being censured for those views, by allowing whistle-blowers to make protected disclosures, and by enabling members of the media and activists to communicate in a secure manner beyond the reach of unlawful government interception.

The key provision under international law regarding the right to privacy is contained in article 17 of the International Covenant on Civil and Political Rights (**ICCPR**). Importantly, sub-article (1) provides that no one shall be subjected to arbitrary or unlawful interference with his (or her) privacy, family, home or correspondence, nor to unlawful attacks on his (or her) honour and reputation. Sub-article (2) goes on to provide that everyone has the right to the protection of the law against such interference or attacks.

In the African context, the African Charter on Human and Peoples’ Rights (**African Charter**) does not contain an express provision on the right to privacy. However, it has been argued that the right can – and should – be read into the African Charter through to the right to respect for life and integrity of the person, the right to dignity, and the right to liberty and security of the person.¹ This argument is based on the approach taken by the African Commission on

---

Human and Peoples’ Rights (African Commission) in Social and Economic Rights Action Centre and Another v Nigeria and the comparative jurisprudence from the Supreme Court of India in Justice KS Puttaswamy (Retd) and Another v Union of India and Others.  

It bears mention that other African regional instruments do recognise the right to privacy. For example, article 10 of the African Charter on the Rights and Welfare of the Child provides that:

“No child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks.”

Additionally, the African Union (AU) Convention on Cyber Security and Personal Data Protection (AU Data Protection Convention) – commonly referred to as the Malabo Convention – recognises in its preamble the commitment of the AU to build the information society and to protect “the privacy of its citizens in their daily or professional lives, while guaranteeing the free flow of information”. However, the Data Protection Convention is not yet in force, as it has received the requisite number of ratifications.

At the domestic level, more than 50 African constitutions, inclusive of amendments and recent reviews, include reference to the right to privacy.  

---

2 Id.

3 Id. The following 52 African constitutions include reference to the right to privacy: articles 46-7 of the Constitution of Algeria (1989); articles 32-4 of the Constitution of Angola (2010); articles 20-1 of the Constitution of Benin (1990); articles 3 and 9 of the Constitution of Botswana (1966); article 6 of the Constitution of Burkina Faso (1991); article 43 of the Constitution of Burundi (2005); Preamble to the Constitution of Cameroon (1972); articles 38, 41 and 42 of the Constitution of Cape Verde (1980); articles 16 and 19 of the Constitution of the Central African Republic (2016); Preamble to the Constitution of the Comoros (2001); articles 29 and 31 of the Constitution of the Democratic Republic of the Congo (2005); articles 20 and 26 of the Constitution of the Republic of the Congo (2015); article 8 of the Constitution of Côte d’Ivoire; articles 12-3 of the Constitution of Djibouti (2010); articles 57-8 of the Constitution of Egypt (2014); article 13 of the Constitution of Equatorial Guinea (1991); article 18 of the Constitution of Eritrea (1997); article 26 of the Constitution of Ethiopia (1994); article(1)(5)-(6) of the Constitution of Gabon (1991); article 23 of the Constitution of The Gambia (1996); article 18 of the Constitution of Ghana (1992); article 12 of the Constitution of Guinea (2010); articles 44 and 48 of the Constitution of Guinea-Bissau (1984); article 31 of the Constitution of Kenya (2010); article 4(f)-(g) of the Constitution of Lesotho (1993); article 16 of the Constitution of Liberia (1986); articles 11-3 of the Constitution of Libya (2011); article 13 of the Constitution of Madagascar (2010); article 21 of the Constitution of Malawi (1994); article 6 of the Constitution of Mali (1992); article 13 of the Constitution of Mauritania (1991); articles 3(c) and 9 of the Constitution of Mauritius (1968); article 24 of the Constitution of Morocco (2011); article 41 of the Constitution of Mozambique (2004); article 13 of the Constitution of Namibia (1990); articles 27 and 29 of the Constitution of Niger (2017); article 37 of the Constitution of Nigeria (1999); article 2 of the Constitution of Rwanda (2003); articles 24-25 of the Constitution of Sao Tome and Principe (1975); articles 13 and 16 of the Constitution of Senegal (2001); article 20 of the Constitution of Seychelles (1993); article 15(c) of the Constitution of Sierra Leone (1991); article 19 of the Constitution of Somalia (2012); article 14 of the Constitution of South Africa (1996); article 22 of the Constitution of South Sudan (2011); article 14(1)(c) of the Constitution of Swaziland (2005); articles 16 and 18 of the Constitution of the United Republic of Tanzania (1977);
Data Protection

Key principles for data protection

Data protection is one of the primary measures through which the right to privacy is given effect. Data protection laws are aimed at protecting and safeguarding the processing of personal information (or personal data). This refers to any information relating to an identified or identifiable natural person – i.e. the data subject – by which the data subject can be identified, directly or indirectly. A data controller, which can typically be either a public or private body, refers to the person or entity responsible for processing the personal information about the data subject.

In addition to giving effect to the right to privacy, data protection laws also typically facilitate a right of access to information. In this regard, most data protection laws provide for data subjects to request, and be given access to, the information being held about them by a controller. This mechanism can enable data subjects to ascertain whether their personal information is being processed in accordance with the applicable data protection laws, and whether their rights are indeed being upheld.

There have already been a number of African states that have enacted data protection laws, and more that are in the process of doing so. In addition to giving effect to the right to privacy, data protection legislation also has a key role to play in facilitating trade amongst states, as many data protection laws restrict cross-border data transfers in circumstances where the state receiving the information does not provide an adequate level of data protection.

Data Protection Africa

Source: [https://dataprotection.africa/](https://dataprotection.africa/)

There are currently approximately 32 countries in Africa that either have an existing or draft data protection framework in place or which make reference to data privacy in existing laws. However, even the countries with a data protection framework in place are facing challenges with resource constraints, delayed implementation or a lack of appointment of the regulatory authorities. Key questions to consider that may differ in different jurisdictions include what constitutes personal information in a particular jurisdiction; the exemptions that may apply; the conditions for the lawful process of data; how that data can be transferred across borders; whether breach notification is required, and if so, what requirements apply. For a full review of the data protection landscape in Africa, visit Data Protection Africa: [https://dataprotection.africa/](https://dataprotection.africa/).

---

article 28 of the Constitution of Togo (1992); article 24 of the Constitution of Tunisia (2014); article 27(1) of the Constitution of Uganda (1995); articles 11(d) and 17 of the Constitution of Zambia (1991); and article 57 of the Constitution of Zimbabwe (2013).
While there may be differences in different jurisdictions, there are a number of key principles that appear in most data protection frameworks. A useful resource in this regard – compiled as a joint initiative of the Internet Society (ISOC) and the AU – are the Personal Data Protection Guidelines for Africa (Data Protection Guidelines).

As set out in the Data Protection Guidelines, the key privacy principles that appear across most data protection frameworks include the following.5

- **Collection limitation**: Personal data must be obtained and processed lawfully, fairly, and, to the extent possible, transparently.
- **Data quality**: Personal data must be accurate at the point of collection, and reasonable steps must be taken to ensure its accuracy is maintained over the period of retention.
- **Purpose specification**: Personal data must be collected only for specified, explicit, and legitimate purposes. Personal data should only be used for such other purposes as are compatible with applicable laws, such as archiving data that is in the public interest, or for scientific research.
- **Use limitation**: Personal data must not be disclosed, made available, or used for other purposes except with the consent of the individual or where authorised by law.
- **Security safeguards**: Personal data should be protected by reasonable security safeguards to maintain its integrity and confidentiality.
- **Openness**: There should be a general policy of openness about developments, practices, and policies with respect to personal data.
- **Individual participation**: Individuals must have the right to obtain information about their personal data held by others. This data must be provided within a reasonable period of time, in a form that is readily intelligible, and at a cost that is not excessive. Data subjects have the right to challenge their data and to have it amended if it is inaccurate, or erased if that is appropriate.
- **Accountability**: Those who collect and process personal data must be able to demonstrate their compliance with these principles.

Another key principle of data protection frameworks is that personal data should not be transferred to a country that does not ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.6

---

5 Data Protection Principles at pp 9-10.
In Maximillian Schrems v Data Protection Commissioner, Mr Schrems – a European citizen – lodged a complaint with the Irish Data Protection Commissioner that some or all of the data that he had provided to Facebook was transferred from Facebook’s Irish subsidiary to servers located in the United States of America (US), where it was processed. As the US does not have a comprehensive data protection law, Mr Schrems argued that the law and practice in the US did not offer sufficient protection against surveillance by the US public authorities, and did not meet the test for adequacy as contemplated under European law.

The Court of Justice of the European Union (CJEU) upheld the claim, noting that the protective rules laid out in the data sharing arrangement between the European Union (EU) and the US (known as the ‘Safe Harbour Agreement’) could be disregarded by the US where they conflicted with national security, public interest and law enforcement requirements of the US. The CJEU held that any legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the right to privacy. Furthermore, the CJEU was of the view that legislation that does not provide for an individual to pursue legal remedies to access one’s personal information, or to have such information rectified or erased, compromises the essence of the right to effective judicial protection.

Accordingly, the CJEU declared the Safe Harbour Decision invalid, with immediate effect. In line with this judgment, the threshold that has been established for determining the adequacy of protection is to ascertain whether it is “essentially equivalent.”

Regional data protection frameworks in Africa

As noted in the Data Protection Guidelines, in considering the relevant data protection framework, it is necessary to understand the African context and the particular characteristics that arise:7

- Significant cultural and legal diversity across the continent, with different privacy expectations.
- Variations in access to technology and online services among member states.
- Sensitivities regarding ethnicity and profiling of citizens without consent.
- Different levels of capability in areas such as technology and technology-related law and governance.
- Risks arising from high dependency on non-African manufacturers and service providers, including the limited ability of African states to influence the behaviour of external service providers, and the potentially increased risk of data misuse where content and services are solely provided by foreign companies.

According to the Data Protection Guidelines, this context presents unique challenges to the enforcement of local data protection laws that may make such enforcement more difficult.

---

7 Data Protection Principles at p 7.
While the AU Data Protection Convention is not yet in force, it still provides useful guidance at the regional level, as well as to states looking to implement data protection frameworks at the domestic level. Chapter II of the AU Data Protection Convention sets out the principles relevant to data protection. As set out in article 8(1), the objective of the AU Data Protection Convention is for each state party to commit itself to establishing a legal framework “aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy with prejudice to the principle of the free flow of personal data.”

Article 13 of the AU Data Protection Convention sets out the following basic principles governing the processing of personal data:

- Principle 1: Principle of consent and legitimacy of personal data processing.
- Principle 2: Principle of lawfulness and fairness of personal data processing.
- Principle 3: Principle of purpose, relevance and storage of processed personal data.
- Principle 4: Principle of accuracy of personal data.
- Principle 5: Principle of transparency of personal data processing.

Articles 16 to 19 of the AU Data Protection Convention set out the rights of data subjects, namely the right to information; the right of access; the right to object; and the right of rectification or erasure. Articles 20 to 23 go on to set out the obligations of personal data controllers, namely the confidentiality obligations; the security obligations; the storage obligations; and the sustainability obligations.

In respect of cross-border data transfers, article 14(6)(a) provides that: “The data controller shall not transfer personal data to a non-Member State of the African Union unless such a State ensures an adequate level of protection of the privacy, freedoms and fundamental rights of the persons whose data are being or are likely to be processed”. Sub-article (b) goes on to provide that the prohibition does not apply if the data controller has requested authorisation for the transfer from the relevant data protection authority before the data has been transferred.

### Processing for journalistic, research, artistic or literary purposes

**Source:** [https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf](https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf)

Article 14(3) of the AU Data Protection Convention provides for a specific exemption that applies to the processing of personal data for journalistic, research, artistic or literary purposes. It provides that: “Personal data processing for journalistic purposes or for the purposes of research or artistic or literary expression shall be acceptable where the processing is solely for literary or artistic expression or for professional exercise of...
Article 14(4) goes on to provide that the provisions of the AU Data Protection Convention “shall not preclude the application of national legislations with regard to the print media or the audio-visual sector, as well as the provisions of the criminal code which provide for the conditions for exercise of the right of reply, and which prevent, limit, compensate for and, where necessary, repress breaches of privacy and damage to personal reputation.”

Extra-territorial application of data protection frameworks in Europe

There are two key European instruments in respect of data protection that have extra-territorial application for African states. The first is the Convention for the Protection of Individuals with regard to the Processing of Personal Data\(^9\) – commonly referred to as Convention 108 – which is an instrument of the Council of Europe (COE). Convention 108 opened for signature on 28 January 1981, and was the first legally binding instrument in the data protection field.\(^10\) The purpose of Convention 108 is to “protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy”.\(^11\) Convention 108 provides for the free flow of personal data between states parties to the Convention.

A key feature of Convention 108 is that, in addition to the members of the COE, it also provides that non-European states may accede to it. For example, in the African context, Cape Verde, Mauritius and Senegal have all acceded to it. This is of relevance for several reasons: it is a recognition of the adequacy of their data protection frameworks; it adds an additional bulwark of protection of persons within those states; and it can serve to facilitate cross-border data transfers between those African states and Europe. Convention 108 remains open for accession to other African states that may meet the necessary requirements.

Modernisation of Convention 108


In May 2018, the COE published Convention 108+, in an effort to update and modernise Convention 108. Key issues for consideration in this regard were the automatic processing of personal data and cross-border data transfers. As noted in the explanatory report to Convention 108+: “In the 35 years that have elapsed since the Convention for the Protection of Individuals with regard to Automated Processing of Personal Data, also known as Convention 108 (hereafter also referred to as “the Convention”) was opened for signature,\(^9\)


\(^{11}\) Article 1 of Convention 108.
the Convention has served as the foundation for international data protection law in over 40 European countries. It has also influenced policy and legislation far beyond Europe’s shores. With new challenges to human rights and fundamental freedoms, notably to the right to private life, arising every day, it appeared clear that the Convention should be modernised in order to better address emerging privacy challenges resulting from the increasing use of new information and communication technologies (IT), the globalisation of processing operations and the ever greater flows of personal data, and, at the same time, to strengthen the Convention’s evaluation and follow-up mechanism.”

The second key instrument is the European Union General Data Protection Regulation 2016/679 (GDPR). The GDPR is applicable to all member states of the EU as of 25 May 2018 and is an effort to harmonise all data protection laws across Europe. As explained in article 1 of the GDPR, its purpose is to lay down rules relating to the protection of natural persons with regard to the processing of personal data, as well as rules relating to the free movement of personal data. In particular, article 1(2) makes clear that the GDPR is intended to protect “fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data”.

Chapter II of the GDPR sets out the following principles:

- Article 5: Principles relating to the processing of personal data.
- Article 6: Lawfulness of processing.
- Article 7: Conditions for consent.
- Article 8: Conditions applicable to a child’s consent in relation to information society services.
- Article 9: Processing of special categories of personal data.
- Article 10: Processing of personal data relating to criminal convictions and offences.
- Article 11: Processing which does not require identification.

The conditions for consent bear special emphasis. Importantly, the data controller bears the burden of demonstrating that the data subject has consented to the processing of his or her personal data. Where written consent is sought, the GDPR provides that this request for consent “shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language” in order for it to be binding. The data subject has the right to withdraw consent at any time, and it is required that it be made as easy to withdraw consent as it is to give consent. Added to this, the GDPR provides that when assessing whether consent is freely given, utmost account must be taken of whether the performance of a contract or provision of a service “is conditional on consent to the processing of personal data that is not necessary for the performance of that contract”.

---

12 Accessible at https://gdpr-info.eu/.
13 Article 7(1) of the GDPR.
14 Article 7(2) of the GDPR.
15 Article 7(3) of the GDPR.
16 Article 7(4) of the GDPR.
A unique and notable inclusion in the GDPR is that it seeks to apply extra-territorially, to data controllers that are not established in the EU, regardless of whether the processing takes place in the EU or not. In this regard, article 3 of the GDPR provides as follows:

“(1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

(2) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
   (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

(3) This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.”

Recital 23 to the GDPR explains that the purpose of this provision is to ensure that natural persons are not deprived of the protection to which they are entitled under the GDPR. In respect of article 3(2)(a) of the GDPR, recital 23 explains as follows:

“In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller’s, processor’s or an intermediary’s website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.”

Recital 24 to the GDPR goes on to provide an explanation of article 3(2)(b) of the GDPR. It explains that: “In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.”
The failure to comply with the GDPR carries with it significant penalties, including administrative fines of up to €20 000 or 4% of the total worldwide annual turnover of the preceding year, whichever is higher.\(^{17}\)

**Representation of data subjects in terms of the GDPR**

Article 80 of the GDPR deals with the representation of data subjects. Article 80(1) provides that a data subject has a right to mandate a not-for-profit body, organisation or association – which has been properly constituted within the law of a member state, has statutory objectives in the public interest and is active in the field of data protection – to exercise the data subject’s rights on his or her behalf. This opens the door for class action litigation to be brought as a result of an infringement of a provision of the GDPR.

Article 80(2) further gives member states the option to allow anybody, organisation or association referred to in article 80(1) to lodge a complaint independently of a data subject’s mandate, if it appears that there has been an infringement of a right as a result of data processing. However, as explained in recital 142, that body, organisation or association may not be allowed to claim compensation on a data subject’s behalf independently of the data subject’s mandate.

**Use of data protection authorities to vindicate the right to privacy**

Data protection frameworks typically provide for the establishment of a data protection authority (DPA) to oversee and enforce the relevant framework. Such DPAs are typically given a range of powers, including to be notified in the event of a data breach, to adjudicate complaints and to impose penalties where a data controller is found to be non-compliant with the data protection framework.

In states with established DPAs, it should be noted that this may be an avenue to vindicate the right to privacy. In the event of a data breach or another infringement of the data protection framework, data subjects may be assisted with lodging complaints to the relevant DPA. This quasi-judicial forum can present a relatively quick and cost-effective remedy for the data subject.

\(^{17}\) Article 83 of the GDPR.
Data Retention

**Report of the UN Human Rights Committee regarding data retention in South Africa**


Section 30(2) of the *South African Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002* (RICA) obliges telecommunications service providers to retain all data for a period prescribed by the relevant executive authority, which may be between a period of three years and five years. The current prescription is three years. This means that all of a person’s personal telecommunications, up to three years past, lie in wait for the state to pry into, if the officials convince a judicial officer to authorise access.

In 2016, in the Human Rights Committee’s concluding observations regarding South Africa’s compliance with the ICCPR, the Human Rights Committee raised concern “about the wide scope of the data retention regime under [RICA]”. The Human Rights Committee therefore recommended that South Africa “should refrain from engaging in mass surveillance of private communications without prior judicial authorization and consider revoking or limiting the requirement for mandatory retention of data by third parties.”

Data retention is typically described as “the process through which governments and businesses (especially telecommunication and internet providers) record and store various data (usually related to individuals).”

“...The practice of data retention involves the gathering and storing of communications data for extended periods for the purpose of future access. Metadata tells the story about your data and answers the who, when, what, and how of a specific communication. Data collected will likely cover a mixture of personally identifiable and non-identifiable information, including traffic data (data about how a communication was transmitted including source, destination, means of transmission, time and location of transmission), subscriber data (data identifying subscribers as provided to the communications service provider) and data specific to the use of the communications service in question (time of use, billing information, amount of data downloaded, redirection services). Data retention serves multiple uses,

---

some of which are commercial and others not. Retention can similarly be voluntary, for instance where the data is kept by a company for its internal uses, or it can be mandated by law for potential access by third parties, in particular by governmental agencies.

While, on the one hand, data retention can be important for crime prevention or criminal investigations, it also gives more power to governments to monitor the public and takes away their rights to online privacy.\textsuperscript{20} The practice of mandating the retention of communications data (or metadata) raises significant privacy, transparency and security concerns. In turn, this may affect the ways in which people exercise their rights online, and poses a risk of leading to self-censorship.

It has been noted that: “Data retention laws are different from country to country, but they ultimately have the same goal: A better grip on the digital world at the expense of privacy and freedom of speech.”\textsuperscript{21} Privacy International explains that the mass retention of individuals’ communications records, outside the context of any criminal investigation or business purpose, “amounts to the compilation of dossiers on each and every one of us, our friends, family and colleagues”.\textsuperscript{22} Privacy International goes on to explain that:

“The potential harms associated with data retention and access are significant. In a context where the gathering and exploitation of data by private companies becomes increasingly privacy intrusive and widespread, data retention poses serious risks to individual privacy and data security. The data opens the door for governments and third parties to make intimate inferences about individuals, to engage in profiling and to otherwise intrude on people’s private lives. If the information is not properly protected there is the potential of unauthorised access to troves of information by third parties, including cyber-criminals.”

Most data protection frameworks provide that data should only be collected for specified, explicit and legitimate purposes and that such data should, in the ordinary course, be deleted when this is no longer the case. Additionally, data ought not to be kept for longer than it is needed. For example, article 5(1)(e) of the GDPR provides that personal data shall be—

“kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes … subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’).”

\begin{flushleft}
\textsuperscript{20} Id.
\textsuperscript{21} Id.
\end{flushleft}
In general, there are two key factors that determine an appropriate data retention period: (i) the purpose for processing the data; and (ii) any legal or regulatory requirements for retaining it. In respect of the latter, various countries have mandatory data retention laws that require telecommunication and internet service providers to retain certain types of data – such as metadata – for stipulated periods of time.

Importantly, there have been at least two significant judgments of the CJEU — Digital Rights Ireland\(^23\) and Tele2 Sverige AB\(^24\) — that have reaffirmed the requirement that all data retention regimes must comply with the principles of legality, necessity and proportionality.\(^25\) Appropriate safeguards are also needed to protect the data that has been retained.

---

**Indefinite retention of DNA, fingerprints and photograph held to be in breach of privacy rights**


In the February 2020 judgment of *Gaughran v United Kingdom* (application no. 45245/15), the matter concerned a complaint about the indefinite retention of data (DNA profile, fingerprints and a photograph) of a man who had a spent conviction for driving with excess alcohol. The European Court of Human Rights (ECtHR) held that there had been a violation of his privacy rights in terms of article 8 of the European Convention on Human Rights (European Convention). The ECtHR underlined that it was not the duration of the retention of data that had been decisive, but the absence of certain safeguards. In the applicant’s case, his personal data had been retained indefinitely without consideration of the seriousness of his offence, the need for indefinite retention, and without any real possibility of review. Noting that the technology being used had been shown to be more sophisticated than that considered by the domestic courts in this case, particularly regarding storage and analysis of photographs, the ECtHR considered that the retention of the applicant’s data had failed to strike a fair balance between the competing public and private interests.

---

**Surveillance**

*Government-led digital surveillance*

The knowledge, or even the perception, of being surveilled can lead to self-censorship. Online surveillance has been a central issue for human rights activists for years, but following the Snowden revelations about the extent and scope of surveillance activities, it has become a pressing global issue. Communications surveillance encompasses the monitoring,
intercepting, collecting, obtaining, analysing, using, preserving, retaining, interfering with, accessing or similar actions taken with regard to information that includes, reflects, arises from or is about a person’s communications in the past, present, or future. This relates to both the content of communications and metadata. In respect of the latter, it has been noted that the aggregation of information – commonly referred to as ‘metadata’ – may give an insight into an individual’s behaviour, social relationships, private preferences and identity. Taken as a whole, it may allow very precise conclusions to be drawn concerning the private life of a person.

African Declaration on Internet Rights and Freedoms

Source: [https://africaninternetrights.org/articles/](https://africaninternetrights.org/articles/)

Principle 9 of the African Declaration on Internet Rights and Freedoms (AfDec) — a civil-society led initiative that has been endorsed by the African Commission on Human and Peoples’ Rights — provides that “[u]nlawful surveillance, monitoring and interception of users’ online communications by state or non-state actors fundamentally undermine the security and trustworthiness of the Internet.” The AfDec goes on to explain that:

“Mass or indiscriminate surveillance of individuals or the monitoring of their communications, constitutes a disproportionate interference, and thus a violation, of the right to privacy, freedom of expression and other human rights. Mass surveillance shall be prohibited by law.

The collection, interception and retention of communications data amounts to an interference with the right to privacy and freedom of expression whether or not the data is subsequently examined or used. In order to meet the requirements of international human rights law, targeted surveillance of online communications must be governed by clear and transparent laws which, at a minimum, comply with the following basic principles: first, communications surveillance must be both targeted and based on reasonable suspicion of commission or involvement in the commission of serious crime; second, communications surveillance must be judicially authorised and individuals placed under surveillance must be notified that their communications have been monitored as soon as practicable after the conclusion of the surveillance operation; third, the application of surveillance laws must be subject to strong parliamentary oversight to prevent abuse and ensure the accountability of intelligence services and law enforcement agencies.

It should also be recognised that for the enjoyment of their right to privacy, individuals must be protected from unlawful surveillance by other individuals, private entities or institutions, including in their place of work or study and in public internet access points.”

General Comment No 16 to the ICCPR provides that “[s]urveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited”. Surveillance – both bulk (or mass) collection of data or targeted collection of data – interferes directly with the privacy and security necessary for freedom of opinion and expression, and must be considered against the three-part test to assess the permissibility of the restriction. In the digital age, ICTs have enhanced the capacity of governments, corporations and individuals to conduct surveillance, interception and data collection, and have meant that the effectiveness in conducting such surveillance is no longer limited by scale or duration.

---

27 General Comment No 16 at para 8.
In a resolution adopted by the United Nations General Assembly (UNGA) on the right to privacy in the digital age, the UNGA emphasised that unlawful or arbitrary surveillance and/or interception of communications, as well as the unlawful or arbitrary collection of personal data are highly intrusive acts, violate the right to privacy, can interfere with the right to freedom of expression and may contradict the tenets of a democratic society, including when undertaken on a mass scale.\(^{28}\) It noted further that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory.\(^{29}\)

### United Nations (UN) Resolution on the Right to Privacy in the Digital Age


The 2016 UN Resolution on the Right to Privacy in the Digital Age calls on states to, among other things:

- Review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law.
- Establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data.
- Provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations.
- Develop or maintain and implement adequate legislation, with effective sanctions and remedies, that protects individuals against violations and abuses of the right to privacy, namely through the unlawful and arbitrary collection, processing, retention or use of personal data by individuals, governments, business enterprises and private organisations.

Surveillance constitutes an obvious interference with the right to privacy. Further, it also constitutes an interference on the right to hold opinions without interference and the right to freedom of expression. With particular reference to the right to hold opinions without interference, surveillance systems, both targeted and mass, may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as search and browsing,

\(^{29}\) Id.
likely deters individuals from accessing information, particularly where such surveillance leads to repressive outcomes.

In order to meet the condition of legality, many states have taken steps to reform their surveillance laws to allow for the powers required to conduct the surveillance activities. For instance, in the judgment of Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others, the High Court of South Africa held that the exercise of bulk surveillance in South Africa was unlawful because of the absence of any empowering legal framework to authorise such surveillance to take place.³⁰

*Necessary and proportionate*

The Necessary and Proportionate Principles are a set of international principles on the application of human rights to communications surveillance.³¹ As explained in the preamble:

> “Privacy is a fundamental human right, and is central to the maintenance of democratic societies. It is essential to human dignity and it reinforces other rights, such as freedom of expression and information, and freedom of association, and is recognised under international human rights law. Communications Surveillance interferes with the right to privacy among a number of other human rights. As a result, it may only be justified when it is prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.

Before public adoption of the Internet, well-established legal principles and logistical burdens inherent in monitoring communications created limits to Communications Surveillance by States. In recent decades, those logistical barriers to surveillance have decreased and the application of legal principles in new technological contexts has become unclear ... Meanwhile, conceptualisations of existing human rights law have not kept up with the modern and changing Communications Surveillance technologies and techniques of the State, the ability of the State to combine and organize information gained from different surveillance technologies and techniques, or the increased sensitivity of the information available to be accessed.

The frequency with which States are seeking access to both communications content and metadata is rising dramatically, without adequate scrutiny. Communications metadata may create a profile of an individual's life, including medical conditions, political and religious viewpoints, associations, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications. Despite the vast potential for intrusion into an individual's life and the chilling effect on political and other associations, laws, regulations activities, powers, or

³¹ Accessible at https://necessaryandproportionate.org/principles. The Necessary and Proportionate Principles were drafted by Access Now, the Electronic Freedom Foundation and Privacy International, and launched at the UN Human Rights Council in 2013. It has since been endorsed by more than 400 organisations around the world.
authorities often afford communications metadata a lower level of protection and do not place sufficient restrictions on how they can be subsequently used by States."

In terms of the principle of necessity, principle 3 explains that surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. As such, surveillance should only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification rests on the state.

According to principle 5, surveillance should be regarded as a highly intrusive act, and in order to meet the threshold of proportionality, the state should be required at a minimum to establish the following information to a competent judicial authority prior to conducting any communications surveillance:

- There is a high degree of probability that a serious crime or specific threat to a legitimate aim has been or will be carried out.
- There is a high degree of probability that evidence relevant and material to such a serious crime or specific threat to a legitimate aim would be obtained by accessing the protected information sought.
- Other less invasive techniques have been exhausted or would be futile, such that the technique used is the least invasive option.
- Information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a legitimate aim alleged.
- Any excess information collected will not be retained, but instead will be promptly destroyed or returned.
- Information will be accessed only by the specified authority and used only for the purpose and duration for which authorisation was given.
- The surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.

Safeguards and oversight

Privacy International sets out the following ten safeguards that should be implemented for any government hacking or surveillance regime:

- **Legality**: Government hacking powers must be explicitly prescribed by law and limited to those strictly and demonstrably necessary to achieve a legitimate aim. That law must be accessible to the public and sufficiently clear and precise to enable persons to foresee its application and the extent of the interference. It should be subject to periodic review by means of a participatory legislative process.

---

32 Principle 5 of the Necessary and Proportionate Principles.
• **Security and integrity of systems**: Prior to carrying out a hacking measure, government authorities must assess the potential risks and damage to the security and integrity of the target system and systems generally, as well as of data on the target system and systems generally, and how those risks and/or damage will be mitigated or corrected. Government authorities must include this assessment in any application in support of a proposed hacking measure. Government authorities must not compel hardware or software manufacturers or service providers to facilitate government hacking, including by compromising the security and integrity of their products and services.

• **Necessity and proportionality**: Prior to carrying out a hacking measure, government authorities must, at a minimum, establish a high degree of probability that: (i) serious crime or act(s) amounting to a specific, serious threat to national security has been or will be carried out; (ii) the system used by the person suspected of committing the serious crime or act(s) amounting to a specific, serious threat to national security contains evidence relevant and material to the serious crime or act(s) amounting to a specific, serious threat to national security interest alleged; and (iii) evidence relevant and material to the serious crime or act(s) amounting to a specific, serious threat to national security alleged will be obtained by hacking the target system.

• **Judicial authorisation**: Prior to carrying out a hacking measure, government authorities must make an application, setting forth the necessity and proportionality of the proposed measure to an impartial and independent judicial authority, who shall determine whether to approve such measure and oversee its implementation. The judicial authority must be able to consult persons with technical expertise in the relevant technologies, who may assist the judicial authority in understanding how the proposed measure will affect the target system and systems generally, as well as data on the target system and systems generally. The judicial authority must also be able to consult persons with expertise in privacy and human rights, who may assist the judicial authority in understanding how the proposed measure will interfere with the rights of the target person and other persons.

• **Integrity of information**: Government authorities must not add, alter or delete data on the target system, except to the extent technically necessary to carry out the authorised hacking measure. They must maintain an independently verifiable audit trail to record their hacking activities, including any necessary additions, alterations or deletions. Where government authorities rely on data obtained through an authorised hacking measure, they must disclose the method, extent and duration of the hacking measure and their audit trail so that the target person can understand the nature of the data obtained and investigate additions, alterations or deletions to information or breaches of the chain of custody, as appropriate.

• **Notification**: Government authorities must notify the person(s) whose system(s) have been subject to interference pursuant to an authorised hacking measure, regardless of where the person(s) reside, that the authorities have interfered with such system(s). Government authorities must also notify affected software and hardware manufacturers and service providers, with details regarding the method, extent and duration of the
hacking measure, including the specific configurations of the target system. Delay in notification is only justified where notification would seriously jeopardise the purpose for which the hacking measure was authorised or there is an imminent risk of danger to human life and authorisation to delay notification is granted by an impartial and independent judicial authority.

- **Destruction and return of data**: Government authorities must immediately destroy any irrelevant or immaterial data that is obtained pursuant to an authorised hacking measure. That destruction must be recorded in the independently verifiable audit trail of hacking activities. After government authorities have used data obtained through an authorised hacking measure for the purpose for which authorisation was given, they must return this data to the target person and destroy any other copies of the data.

- **Oversight and transparency**: Government authorities must be transparent about the scope and use of their hacking powers and activities, and subject those powers and activities to independent oversight. They should regularly publish, at a minimum, information on the number of applications to authorise hacking approved and rejected; the identity of the applying government authorities; the offences specified in the applications; and the method, extent and duration of authorised hacking measures, including the specific configurations of target systems.

- **Extraterritoriality**: When conducting an extraterritorial hacking measure, government authorities must always comply with their international legal obligations, including the principles of sovereignty and non-intervention, which express limitations on the exercise of extraterritorial jurisdiction. Government authorities must not use hacking to circumvent other legal mechanisms – such as mutual legal assistance treaties or other consent-based mechanisms – for obtaining data located outside their territory. These mechanisms must be clearly documented, publicly available, and subject to guarantees of procedural and substantive fairness.

- **Effective remedy**: Persons who have been subject to unlawful government hacking, regardless of where they reside, must have access to an effective remedy.

---

**Impugned provisions of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (RICA) declared unconstitutional**


In the case of *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others*, the High Court of South Africa declared various provisions of RICA to be unconstitutional for its failure to provide for appropriate safeguards. The order included the following:
RICA, including sections 16(7), 17(6), 18(3)(a), 19(6), 20(6), 21(6) and 22(7) thereof, is inconsistent with the Constitution and accordingly invalid to the extent that it fails to prescribe procedure for notifying the subject of the interception.

RICA, including the definition of ‘designated judge’ in section 1, is inconsistent with the Constitution and accordingly invalid to the extent that it fails to prescribe an appointment mechanism and terms for the designated judge which ensure the designated judge's independence.

RICA, including sections 16(7) thereof, is inconsistent with the Constitution and accordingly invalid to the extent that it fails to adequately provide for a system with appropriate safeguards to deal with the fact that the orders in question are granted ex parte.

RICA, especially sections 35 and 37, are inconsistent with the Constitution and accordingly invalid to the extent that the statute itself fails to prescribe proper procedures to be followed when state officials are examining, copying, sharing, sorting through, using, destroying and/or storing the data obtained from interceptions.

Sections 16(5), 17(4), 19(4), 21 (4) (a), and 22(4) (b) of RICA are inconsistent with the Constitution and accordingly invalid to the extent that they fail to address expressly the circumstances where a subject of surveillance is either a practising lawyer or a journalist.

It is declared that the bulk surveillance activities and foreign signals interception undertaken by the National Communications Centre are unlawful and invalid.

On 25 February 2020, the Constitutional Court of South Africa heard an application for confirmation of the High Court order, as well as an application for leave to appeal by the state. At the time of writing, the Constitutional Court has not yet handed down its judgment.

Covert recordings

There are various domestic law and international standards that require that individuals be notified of covert recordings, including video surveillance. However, there is no consistent position on this issue. There are two key recent decisions of the Grand Chamber of the ECtHR that are relevant in this regard:

- Antović and Mirković v Montenegro: This case concerned an invasion of privacy complaint by two professors at the University of Montenegro’s School of Mathematics after video surveillance had been installed in areas where they taught. They stated that they had had no effective control over the information collected and that the surveillance had been unlawful. The domestic courts rejected a compensation claim however, finding that the question of private life had not been at issue as the auditoriums where the applicants taught were public areas. The ECtHR held that there had been a violation

---


of article 8 of the European Convention, finding that the camera surveillance had not been in accordance with the law. It first rejected the government’s argument that the case was inadmissible because no privacy issue had been at stake as the area under surveillance had been a public, working area. In this regard, the ECtHR noted in particular that it had previously found that private life might include professional activities and considered that was also the case with the applicants. Article 8 of the European Convention was therefore applicable. On the merits of the case, the ECtHR then found that the camera surveillance had amounted to an interference with the applicants’ right to privacy and that the evidence showed that that surveillance had violated the provisions of domestic law. According to the ECtHR, the domestic courts had never even considered any legal justification for the surveillance because they had decided from the outset that there had been no invasion of privacy.

- **Ribalda and Others v Spain**. This case concerned the covert video-surveillance of employees which led to their dismissal. The applicants complained about the covert video-surveillance and the Spanish courts’ use of the data obtained to find that their dismissals had been fair. The applicants who signed settlement agreements also complained that the agreements had been made under duress owing to the video material and should not have been accepted as evidence that their dismissals had been fair. The Grand Chamber held that there had been no violation of article 8 of the European Convention in respect of the five applicants. It found in particular that the Spanish courts had carefully balanced the rights of the applicants — supermarket employees suspected of theft — and those of the employer, and had carried out a thorough examination of the justification for the video-surveillance. A key argument made by the applicants was that they had not been given prior notification of the surveillance, despite such a legal requirement, but the ECtHR found that there had been a clear justification for such a measure owing to a reasonable suspicion of serious misconduct and to the losses involved, taking account of the extent and the consequences of the measure. The ECtHR concluded that, in the present case, the domestic courts had thus not exceeded their power of discretion or margin of appreciation in finding the monitoring proportionate and legitimate.

In respect of the media, considerations of public interest and the public status of individuals are key determinants in whether information should be published. This was affirmed, for instance, in the case **Radio Twist v Slovakia**, where the ECtHR had cause to consider the unlawful recording of a telephone call that had been broadcast on the radio. The recording was of a conversation amongst several senior members of government discussing issues around the privatisation of an insurance company. The recording had not been made by the radio station, but had been dropped in its mailbox. The ECtHR had particular regard to the context and content of the conversation being clearly political in nature, and the subject-matter of the conversation being on a matter of general interest. As to whether the recording was illegal, the ECtHR stated that it was not convinced that the mere fact that the recording had been obtained by a third party contrary to the law justified the applicant being deprived of its

38 Application No. 62202/00, 8 November 2005, accessible at http://hudoc.echr.coe.int/eng?i=001-71431.
39 Id. at para 58.
right to freedom of expression.\textsuperscript{40} The ECtHR therefore held that the radio station had not violated the rights of the persons who were recorded.

Principle 12(a) of the Global Principles lists the following factors to take into consideration in balancing the rights to freedom of expression and privacy, relevant in determining whether to publish: the extent to which the publication at issue contributes to a debate of public interest; the degree of notoriety or vulnerability of the person affected; the subject covered by the publication and the extent of the private nature of the information at issue; the prior conduct of the person concerned; the content, form, and consequences of the publication; the way in which the information was obtained; the intent of the individual or entity disseminating the information at issue, and in particular whether it was malicious; and the extent to which the individual whose privacy is at issue is a public figure.\textsuperscript{41}

Furthermore, when dealing with photographs, video footage or sound recordings, regard should also be had to whether this was taken voluntarily and with consent. It has been suggested that privacy-invasive techniques, such as hidden cameras or undercover reporting, should only be permitted where there is an overriding public interest in the dissemination of the information sought or discovered which could not have been obtained by less invasive means, and efforts have been made to address the privacy concerns to minimise the interference.\textsuperscript{42}

**Collection of Biometric Data and Facial Recognition**

The collection and retention of biometric data presents a unique set out of concerns. As biometric data can remain relevant for the course of a person’s life, the security of this data is paramount. Biometric data breaches seriously affect individuals in a number of ways, whether identity theft or fraud, financial loss or other damage.

On 30 January 2020, Kenya’s high court handed down judgment on the validity of NIIMS, which includes the collection of biometric information. The court ruled that the implementation of NIIMS should not continue without further legislation to guarantee the security of biometric data and to ensure that the system is not exclusionary.

\textsuperscript{40} Id. at para 62.  
\textsuperscript{42} Principle 12(c) of the Global Principles of Freedom of Expression and Privacy.
As noted by Privacy International, “[i]t is essential that the government meaningfully addresses the issues raised by the Court, and that the solutions presented genuinely address the Court’s concerns.”

Facial recognition is one form of biometric system that is gaining increased prevalence and being used for general surveillance. Facial recognition technology uses cameras loaded with software to match live footage of people in public with images on a ‘watch list’. As noted by Privacy International, facial recognition cameras are far more intrusive than regular CCTV: they scan distinct, specific features of your face, such as face shape, to create a detailed map of it – “which means that being captured by these cameras is like being fingerprinted, without your knowledge or consent”.

**Facial recognition in practice in the United Kingdom**


“Facial recognition technology has been trialled by UK police forces. A trial was conducted by Leicestershire Police at a music festival in 2015. In August 2016, the Metropolitan Police Service used automated facial recognition technology to monitor and identify people at the Notting Hill Carnival. This technology, which is classed by police forces as “overt surveillance”, works by scanning the faces of those passing by overt cameras and then comparing the images against a database of images populated by the police force in question. At the Notting Hill Carnival, the database was populated with images of individuals who were forbidden from attending Carnival, as well as individuals who the police believed may attend Carnival to commit offences. The combination of image databases and facial recognition technology could be used to track people’s movements by combining widespread CCTV and access to a huge searchable database of facial images.”

In this regard, unlike many other biometric systems, facial recognition can be used for general surveillance in combination with public video cameras, and it can be used in a passive way that doesn’t require the knowledge, consent, or participation of the subject. As noted by the American Civil Liberties Union, the biggest danger is that this technology will be used for general, suspicion-less surveillance systems. For example, most motor vehicle agencies possess high-quality photographs of most citizens, which could be a natural source for facial recognition programmes and could easily be combined with public surveillance or other cameras in the construction of a comprehensive system of identification and tracking.

---


45 Id.

Interpol has noted that computerised facial recognition is a relatively new technology, being introduced by law enforcement agencies around the world in order to identify persons of interest, including criminals, fugitives and missing persons. The Interpol Facial Recognition System contains facial images received from more than 160 countries, and coupled with an automatic biometric software application, the system is capable of identifying or verifying a person comparing and analysing patterns, shapes and proportions of their facial features and contours. Unlike fingerprints and DNA, which do not change during a person’s life, facial recognition has to take into account different factors, such as ageing, plastic surgery, cosmetics, the effects of drug abuse or smoking, and the pose of the subject. However, the use of facial recognition technology raises serious concerns. According to a report published in the Washington Post, a recent study in the US, conducted by the National Institute of Standards and Technology, found “empirical evidence” that most of the facial recognition algorithms exhibit “demographic differentials that can worsen their accuracy based on a person’s age, gender or race. Some of the specific findings included the following:

- Facial-recognition systems misidentified people of colour more often than white people.
- Middle-aged white men generally benefited from the highest accuracy rates.
- Asian and African American people were up to 100 times more likely to be misidentified than white men, depending on the particular algorithm and type of search.
- Native Americans had the highest false-positive rate of all ethnicities.
- The faces of African American women were falsely identified more often in the kinds of searches used by police investigators, where an image is compared to thousands or millions of others in hopes of identifying a suspect.
- Women were more likely to be falsely identified than men, and the elderly and children were more likely to be misidentified than those in other age groups.

Privacy International notes that the use of facial recognition technology impacts on the exercise of at least the following rights:

- **Privacy**: According to Privacy International, “[t]he use of facial recognition in public spaces makes a mockery of our privacy rights”. It is a disproportionate crime-fighting technique, as it scans the face of every person who passes by the camera, whether or not they are suspected of any wrongdoing. The biometric data that it collects can be as uniquely identifying as DNA or a fingerprint, and is typically done without consent or knowledge of the data subject.

---

48 Id.
49 Id.
51 Id.
• **Freedom of expression:** Being watched and identified in public spaces is likely to lead us to change our behaviour, limiting where we go, what we do and with whom we engage. For example, persons might be unwilling to participate in a particular protest action if facial recognition is being used in the area.

• **Equality and non-discrimination:** It has been found that facial recognition software is more likely to misidentify women and black people. There are also concerns that the police use facial recognition to target particular communities.

The roll-out of facial recognition technology is often done without any empowering legal framework to authorise it, and is arguably a disproportionate limitation on the right to privacy and other associated rights. In this regard, if challenged, there is a strong case to be made that the use of facial recognition technology, even for security purposes, would not meet the threshold of the three-part test for a justifiable limitation.

**Encryption and Anonymity on the Internet**

*The interplay between encryption and anonymity*

Encryption and anonymity are necessary tools for the full enjoyment of digital rights and enjoy protection by virtue of the critical role that they play in securing the rights to freedom of expression and privacy. As described by the United Nations Special Rapporteur (UNSR) on Freedom of Expression: 53

“Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments. Where States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities. Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment. The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one’s gender, religion, ethnicity, national origin or sexuality. Artists rely on encryption and anonymity to safeguard and protect their right to expression, especially in situations where it is not only the State creating limitations but also society that does not tolerate unconventional opinions or expression.”

Encryption and anonymity are especially useful for the development and sharing of opinions online, particularly in circumstances where persons may be concerned that their

---

communications may be subject to interference or attack by state or non-state actors. These are therefore specific technologies through which individuals may exercise their rights. Accordingly, restrictions on encryption and anonymity must meet the three-part test to justify the restriction.

According to the UNSR on Freedom of Expression, while encryption and anonymity may frustrate law enforcement and counter-terrorism officials and complicate surveillance, state authorities have generally failed to provide appropriate public justification to support the restriction or to identify situations where the restriction has been necessary to achieve a legitimate goal. The UNSR on Freedom of Expression has therefore called on states to promote strong encryption and anonymity, and noted that decryption orders should only be permissible when it results from transparent and publicly-accessible laws applied solely on a targeted, case-by-case basis to individuals (not to a mass of people), and subject to a judicial warrant and the protection of due process rights of individuals.

Encryption

Encryption refers to a mathematical process of converting messages, information or data into a form unreadable by anyone except the intended recipient, and in doing so protects the confidentiality and integrity of content against third party access or manipulation. With “public key encryption” – the dominant form of end-to-end security for data in transit – the sender uses the recipient’s public key to encrypt the message and its attachments, and the recipient uses her or his own private key to decrypt them. It is also possible to encrypt data at rest that is stored on one’s device, such as a laptop or hard drive.

Outright prohibitions on the individual use of encryption technology disproportionately restricts the right to freedom of expression as it deprives all online users in a particular jurisdiction of the right to carve out a space for opinion and expression, without any particular claim of the use of encryption being for unlawful ends. Likewise, state regulation of encryption may be tantamount to a ban, for example through requiring licences for encryption use, setting weak technical standards for encryption or controlling the import and export of encryption tools.

Requirements for cryptography providers in terms of the Electronic Communications and Transactions Act, 2002


Chapter V of the South African Electronic Communications and Transactions Act, 2002 (ECTA) sets out the requirements for cryptography providers. Section 29 of ECTA provides

54 Id at para 36.
55 Id. at paras 59-60.
56 Id at para 7.
57 Id.
58 Id.
59 Id at para 40.
60 Id at para 41.
It should further be noted that some states have implemented – or proposed implementing – so-called ‘back door access’ in commercially available products, forcing developers to install weaknesses that allow government authorities access to encrypted communications. While the states supporting such measures typically claim that a legal framework is necessary to intercept the content of encrypted communications, the UNSR on Freedom of Expression notes that such states have failed to demonstrate that criminal or terrorist use of encryption serves an insuperable barrier to law enforcement objectives.\(^{61}\) Creating an intentional mechanism to allow state access would inevitably undermine the security of all users online.\(^{62}\)

There is a key role for encryption to play in data protection. It has been noted that: “Companies can reduce the probability of a data breach and thus reduce the risk of fines in the future, if they chose to use encryption of personal data. The processing of personal data is naturally associated with a certain degree of risk. Especially nowadays, where cyber-attacks are nearly unavoidable for companies above a given size. Therefore, risk management plays an ever-larger role in IT security and data encryption is suited, among other means, for these companies.”\(^{63}\)

### Encryption and the GDPR


“The [GDPR] also recognizes these risks when processing personal data and places the responsibility on the controller and the processor in Art. 32(1) of the General Data Protection Regulation to implement appropriate technical and organisational measures to secure personal data. The GDPR deliberately does not define which specific technical and organisational measures are considered suitable in each case, in order to accommodate individual factors. However, it gives the controller a catalogue of criteria to be considered when choosing methods to secure personal data. Those are the state of the art, implementation costs and the nature, scope, context and purposes of the processing. In addition to these criteria, one always has to consider the severity of the risks to the rights and freedoms of the data subject and how likely those risks could manifest. This basically boils down to the following: The higher the risks involved in the data processing and the more likely these are to manifest, the stronger the taken security measures have to be and the more measures must be taken. Encryption as a concept is explicitly mentioned as one possible technical and organisational measure to secure data in the list of Art. 32(1) of the GDPR, for the establishment and maintenance of a register of cryptography providers, as well as the particulars that must be recorded in the register, including the name and address of the cryptography provider, as well as a description of the type of cryptography service or product being provided. Section 29(3) provides that a cryptography provider “is not required to disclose confidential information or trade secrets in respect of its cryptography products or services.”

61 Id at para 42.
62 Id.
which is not exhaustive. Again, the GDPR does not mention explicit encryption methods to accommodate for the fast-paced technological progress. When choosing a method one must also apply the criteria catalogue above. To answer the question of what is currently considered “state of the art” data protection officers usually rely on the definitions set out in information security standards like ISO/IEC 27001 or other national IT-security guidelines.”

Encryption of personal data has additional benefits for controllers or processors; for example, the loss of a state of the art encrypted mobile storage medium which holds personal data may not necessarily be considered a data breach that must be reported to the DPA. In addition, if there is a data breach, the authorities must positively consider the use of encryption in their decision on whether and what amount a fine is imposed as per article 83(2)(c) of the GDPR.

In April 2018, the DPAs of the EU, represented in the Article 29 Working Party (WP29), published a statement regarding encryption and its impact on the protection of individuals with regard to the processing of their personal data in the EU. In the statement, the WP29 expressed the view that “the availability of strong and efficient encryption is a necessity in order to guarantee the protection of individuals with regard to the confidentiality and integrity of their data which are the elementary underpinning of the digital economy. Any obligation aiming at reducing the effectiveness of those techniques in order to allow law enforcement access to encrypted data could seriously harm the privacy of European citizens”.

WP29 went on to note three key points:

- Strong encryption is required to ensure a secure, free flow of data between citizens, businesses and governments: The WP29 noted that properly-implemented encryption using appropriate algorithms offers a reasonable guarantee that activities — like buying goods online, filing taxes, using banking services, sending or receiving emails or making an appointment with a physician — can be done securely. According to the WP29, without encryption, individuals’ privacy and security can be compromised every time they wish to undertake those everyday activities. It was noted further that the use of encryption techniques as a means of guaranteeing confidentiality and integrity of data and user authentication has become “an indispensable prerequisite for the normal functioning of these infrastructures and of the digital services offered over them, and is now used by many data controllers”. The WP29 described encryption as “absolutely necessary and irreplaceable for guaranteeing strong confidentiality and integrity when data are transferred across open networks like the Internet, or stored in mobile devices like smartphones”. According to the WP29, encryption should ideally always cover the entire communication, from the device of the sender to that of the recipient, commonly referred to as end-to-end-encryption. The WP29 also noted that there is a public interest in the implementation of encryption: “Securing personal data in transit and at rest is a

64 Id.
65 Id.
67 Id at p 1.
68 Id at pp 1-3.
cornerstone of the trust we all need for digital services, so as to enable innovation and growth for our digital economy.”

- Backdoors and master keys deprive encryption of its utility and cannot be used in a secure manner: The WP29 noted the argument that, because encryption may be used to conceal criminal activities, some consider that the need for law enforcement to access the data of suspected criminals can be satisfied by implementing ‘back doors’ – i.e. vulnerabilities secretly implemented in a particular software by its developer – or ‘master keys’ – i.e. keys allowing the decryption of every message encrypted with specific software – in encryption software. However, as explained by the WP29, “the mathematical foundation of cryptology does not provide the basis for a secure backdoor, and numerous examples in history have shown that master keys and backdoors cannot be kept secure, even by major law enforcement agencies or by companies specialized in key management”. According to the WP29, because encryption software is used on a worldwide scale, this would require backdoors and master keys to be exchanged between law enforcement agencies on a worldwide scale, which would lead to their widespread dissemination and thus increase the risks of them being compromised. The WP29 also notes in this regard that: “Without strong and efficient encryption, data of citizens, businesses and governments are at risk. Given the importance of the security of everyday services – upon which our individual lives, businesses and governments increasingly rely – any decrease in the protection offered by encryption will lead to even greater damages than that which law enforcement access to encrypted data might aim to prevent.” The WP29 also raises concern that imposing backdoors and master keys on law-abiding citizens and organisations would not be an effective measure against criminals, as criminals would use or adapt to the state of the art encryption to protect their data, which in turn would only harm the honest citizen by making their data vulnerable.

- Law enforcement agencies already have a number of legal powers and targeted tools to address the challenge of encryption, allowing them to access the data they need to investigate and prosecute criminals: According to the WP29, law enforcement agencies can be legally empowered in other ways to obtain access to data otherwise encrypted, including personal data, for investigations in targeted circumstances. While these powers may raise serious privacy concerns in themselves, the WP29 argues that they appear more proportionate and less dangerous than backdoors or master keys.

Based on the above, the WP29 made the following findings and recommendations:

- The availability of strong and trusted encryption is a necessity in the modern digital world. Such technologies contribute in an irreplaceable way to our privacy and to the secure and safe functioning of our societies.

- Encryption must remain standardised, strong and efficient, which would no longer be the case if providers were compelled to include backdoors or provide master keys. Whatever the technical solution, it can never be safe to compel encryption providers to include master keys and backdoors in their software.
• Law enforcement agencies already have access to vast quantities of data via their existing powers. Such access must remain proportionate and targeted. They should focus on improving their capabilities to interpret that data to investigate and prosecute criminals.

Advice on how to implement encryption


The ICO recommends the following measures when implementing encryption:

• When implementing encryption, it is important to consider four things: choosing the right algorithm, choosing the right key size, choosing the right software, and keeping the key secure.
• Over time, vulnerabilities may be discovered in encryption algorithms that can eventually make them insecure. You should regularly assess whether your encryption method remains appropriate.
• It is important to ensure that the key size is sufficiently large to protect against an attack over the lifetime of the data. You should therefore assess whether your key sizes remain appropriate.
• The encryption software you use is also crucial. You should ensure that any solution you implement meets current standards, such as FIPS 140-2 and FIPS 197.
• Advice on appropriate encryption solutions is available from a number of organisations.

You should also ensure that you keep your keys secure, and have processes in place to generate new keys when necessary to do so.

Anonymity

Encryption is a tool that can be used to contribute to one’s anonymity online. Anonymity can be defined either as acting or communicating without using or presenting one’s name or identity, or as acting or communicating in a way that protects the determination of one’s name or identity, or using an invented or assumed name that may not necessarily be associated with one’s legal or customary identity. Anonymity may be distinguished from pseudo-anonymity: the former refers to taking no name at all, whilst the latter refers to taking an assumed name.69

69 Id.
Anonymity has been recognised for the important role it plays in safeguarding and advancing privacy, free expression, political accountability, public participation and debate. As explained by the American Civil Liberties Union (ACLU):71

“The right to remain anonymous is a fundamental component of our right to free speech, and it applies every bit as much in the digital world as it does in the physical one. In the words of the U.S. Supreme Court in McIntyre v. Ohio Elections Commission, “Anonymity is a shield from the tyranny of the majority.”

Unfortunately, the right to remain anonymous has been under steady attack in the online world. Governments and corporations have attempted to unmask unpopular speakers through subpoenas directed at the websites they visit.”

---

**Anonymity as an enabler of fundamental rights**

Source: Association for Progressive Communications (APC), 'The right to freedom of expression and the use of encryption and anonymity in digital communications', February 2015, accessible at https://www.apc.org/sites/default/files/APC%20submission%20to%20SR%20FOEX_20150211_0.pdf

“Anonymity is also inextricably linked to the right to privacy. An individual cannot have a reasonable expectation that his or her privacy is being protected without the ability to control what information is shared about them and how that information is used. Lack of privacy, or even perceived lack of privacy, is understood to have a chilling effect on freedom of expression, leading to self-censorship.

…

Additionally, anonymity is an important enabler of the right to freedom of association and assembly online and the right to be free from discrimination. The relative anonymity that the internet offers enables individuals and minority groups, among others, to associate on sensitive matters such as sexual orientation or religion. Anonymity provides an enabling environment for people to form relationships and seek support for problems that have a social stigma like drug addiction, illnesses such as HIV/AIDS, or sexual abuse. It also allows people to engage in online association based on identities or beliefs that are illegal in some countries, like LGBT groups, political opposition, or religious minorities”.

A number of courts have protected anonymity, both of individual users and of journalistic sources. However, there are also a number of states that prohibit or interfere with anonymity online. In Brazil, for example, anonymity is prohibited by article 5 of the Federal Constitution, which states that “free expression of thought is assured, prohibiting anonymity,” without

---

specifying in which situations this should apply.\textsuperscript{72} Although this restriction was designed to prevent individuals from offending and causing damage to the honour and image of third parties, without leaving any trace for identification, it has been generating confusion and is being used to limit the right to privacy and freedom of expression online and offline.\textsuperscript{73}

Mandatory SIM card registration is a commonplace example that requires real-name registration for online activity.\textsuperscript{74} In this regard, mandatory SIM card registration laws typically require that people provide personal information, including a valid identity document or biometrics, before they can purchase or activate a prepaid SIM card for their mobile device.\textsuperscript{75} As noted by Privacy International, “[p]repaid SIM card use and mandatory SIM card registration laws are especially widespread in African countries: these two factors can allow for a more pervasive system of mass surveillance of people who can access pre-paid SIM cards, as well as exclusion from important civic spaces, social networks, and education and health care for people who cannot.”\textsuperscript{76} As of February 2019:\textsuperscript{77}

- Two countries had not mandated SIM card registration and were not considering doing so: Cabo Verde and Comoros.
- Namibia was considering SIM card registration.
- The state of SIM card registration in Djibouti was inconclusive.

Mandatory SIM card registration severely undermines the ability to be anonymous online. It has been explained that: “If almost every mobile device has its SIM card registered to a particular person, and the government can get access to that mobile subscriber information, the people who own and use such devices can be more easily tracked and monitored. Not all people with mobile devices may fall equally under the watchful eye of such surveillance systems: people advocating for change, people who disagree with the government’s policies, religious or ethnic minorities, journalists, and human rights defenders are particularly vulnerable.”\textsuperscript{78}

\textsuperscript{72} APC, ‘The right to freedom of expression and the use of encryption and anonymity in digital communications’, February 2015, accessible at https://www.apc.org/sites/default/files/APC%20submission%20to%20SR%20FOEX_20150211_0.pdf.
\textsuperscript{73} Id.
\textsuperscript{74} Id at paras 49-52.
\textsuperscript{76} Id.
\textsuperscript{77} Id.
\textsuperscript{78} Id.
Anonymity is especially critical in repressive environments in which certain types of protected expression are outlawed, and lack of anonymity could lead to criminal charges or other consequences. Attempts to ban anonymous speech have particularly been seen during times of protest as a measure aimed at protestors and activists.

Intermediary liability is again of concern in relation to anonymous users, as some states have moved towards imposing responsibilities on internet service providers (ISPs) and media platforms to regulate online comments by anonymous users. For instance, in Delfi v Estonia, the ECtHR upheld an Estonian law that imposes liability on a media platform for anonymous defamatory statements posted on its site. As has previously been argued by MLDI, a court should only order an ISP to disclose user data where:

- An applicant is able to demonstrate to a sufficient degree that a wrongful act has been committed against them, and that the information is sought to enable them to seek redress for that wrongful act;
- The anonymous user has been notified, and has had an opportunity to respond to the application;
- There is no less restrictive means of obtaining the information sought; and
- The applicant’s interest in disclosure has been sufficiently balanced against the rights to freedom of expression and privacy.

### Importance of anonymity online

Source: Financial Times, ‘When online anonymity is a good thing’, 10 October 2018, accessible at [https://www.ft.com/content/f8813f6e-cb54-11e8-9fe5-24ad351828ab](https://www.ft.com/content/f8813f6e-cb54-11e8-9fe5-24ad351828ab)

“Anonymity remains one of the best features of life online. What you say and do becomes more important than who you are. The developer(s) of bitcoin is (are?) still known only by the presumed alias Satoshi Nakamoto. Twitter handles, Reddit usernames and YouTube comments still do not require real names. All have had their own problems with offensive commentary, but it is not clear that anonymity is the real cause. Think of Facebook, which has always gone out of its way to verify identities and where discussions are still not known for their civility.

By contrast, withholding real names may appear the sort of thing a troublemaker would do — but can end up enforcing social pressures more acutely. In 2016, Guanxiong Huang and Kang Li at Michigan State University analysed academic investigations into group

---

80 Id. at para 53.
communications and found that people seemed more sensitive to social norms when they could not rely on parts of their identity (job title, age, location etc) they would usually reach for during group conversations.

The real difference appears to lie in the way that we talk in person versus how we communicate via a computer. Screens, not anonymity, could be the real disinhibitors.”

Source Protection and the Protection of Journalistic Materials

The protection of journalistic sources is central to the ability of journalists to properly investigate stories, as well as for the protection of individuals and whistleblowers who provide information to them. Compelling the disclosure of sources has a chilling effect on freedom of speech and media freedom, in addition to hindering the free flow of information.

In this regard, General Comment No. 34 to the ICCPR provides that states parties “should recognise and respect that element of the right of freedom of expression that embraces the limited journalistic privilege not to disclose sources.” Furthermore, principle XV of the Declaration of Principles on Freedom of Expression in Africa deals with the issue of protection of sources by providing as follows:

“Media practitioners shall not be required to reveal confidential sources of information or to disclose other material held for journalistic purposes except in accordance with the following principles:
- the identity of the source is necessary for the investigation or prosecution of a serious crime, or the defence of a person accused of a criminal offence;
- the information or similar information leading to the same result cannot be obtained elsewhere;
- the public interest in disclosure outweighs the harm to freedom of expression; and
- disclosure has been ordered by a court, after a full hearing.”

It is important to note that the protection of sources has acquired new significance in the digital age in the context of its intersection with the right to privacy of communications. The technological advances in the world today has made surveillance, often justified as necessary for the protection of national security, a problem for the protection of sources. The Secretary-General of the UN has noted surveillance activities can have a chilling effect on media freedom and renders it more difficult to communicate with sources and share and develop ideas, which may lead to self-censorship. Similarly, the UNGA – in its resolution on the safety of

---

84 Id.
85 Id at p 124.
86 Id at p 124.
journalists – emphasised that journalists in the digital age are particularly vulnerable to becoming targets of unlawful or arbitrary surveillance and/or interception of communications in violation of their rights to privacy and freedom of expression. In this regard, it goes on to note that encryption and anonymity tools have become vital to journalists to secure their communications and protect the confidentiality of their sources.

**The right to source protection in South Africa**

Source: [http://www.saflii.org/za/cases/ZAGPJHC/2012/71.html](http://www.saflii.org/za/cases/ZAGPJHC/2012/71.html)

In *Bosasa Operations (Pty) Ltd v Basson and Another*, the South Africa High Court established a general proposition that journalists are not required to reveal their sources, subject to certain exceptions. The court stated in this regard that: “If indeed freedom of the press is fundamental and *sine qua non* for democracy, it is essential that in carrying out this public duty for the public good, the identity of their sources should not be revealed, particularly, when the information so revealed, would not have been publicly known. This essential and critical role of the media, which is more pronounced in our nascent democracy, founded on openness, where corruption has become cancerous, needs to be fostered rather than denuded.”

Surveillance activities carried out against journalists have the risk of fundamentally undermining the source protection to which journalists are otherwise entitled. According to principle 9 of the Global Principles on the Protection of Freedom of Expression and Privacy – published by ARTICLE 19 – the following principles apply to the 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…;
   (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
```


89 Id at para 38.
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.”

Further to this, as set out by the United Nations Educational, Scientific and Cultural Organization (UNESCO), a robust and comprehensive source protection framework would encompass the need to:90

- Recognise the value to the public interest of source protection, with its legal foundation in the right to freedom of expression (including press freedom), and to privacy. These protections should also be embedded within a country’s constitution and/or national law.
- Recognise that source protection should extend to all acts of journalism and across all platforms, services and mediums (of data storage and publication), and that it includes digital data and meta-data.
- Recognise that source protection does not entail registration or licensing of practitioners of journalism.
- Recognise the potential detrimental impact on public interest journalism, and on society, of source-related information being caught up in bulk data recording, tracking, storage and collection.
- Affirm that State and corporate actors (including third-party intermediaries), who capture journalistic digital data must treat it confidentially (also acknowledging the desirability of the storage and use of such data being consistent with the general right to privacy).
- Shield acts of journalism from targeted surveillance, data retention and handover of material connected to confidential sources.
- Define exceptions to all the above very narrowly, so as to preserve the principle of source protection as the effective norm and standard.
- Define exceptions as needing to conform to a provision of “necessity” and “proportionality” — in other words, when no alternative to disclosure is possible, when there is a greater public interest in disclosure than in protection, and when the terms and extent of disclosure still preserve confidentiality as much as possible.
- Define a transparent and independent judicial process with appeal potential for authorised exceptions, and ensure that law-enforcement agents and judicial actors are educated about the principles involved.
- Criminalise arbitrary, unauthorised and wilful violations of confidentiality of sources by third-party actors.
- Recognise that source protection laws can be strengthened by complementary whistleblower legislation.

UNESCO has further noted that there is a particular gender dimension that arises in respect of source protection in the digital age. Women journalists face additional risks in the course of their work – both on- and offline: in the physical realm, these risks include sexual harassment, physical assault and rape, which may limit their physical mobility; and the digital sphere, acts of harassment and threats of violence are rampant.\textsuperscript{91} Similarly, female sources face increased risks when acting as whistleblowers or confidential informants.\textsuperscript{92} As such, women journalists need to be able to rely on secure, non-physical forms of communications with their sources, in particular secure digital communications, to be able to engage with their sources.\textsuperscript{93}

\section*{Digital safety and security are paramount for both female journalists and sources}


“Women journalists need to be able to rely on secure digital communications to ensure that they are not at increased risk in conflict zones, or when working on dangerous stories, such as those about corruption and crime. The ability to covertly intercept and analyse journalistic communications with sources increases the physical risk to both women journalists and their sources in such contexts. Encrypted communications and other defensive measures are therefore of great importance to ensure that their movements are not tracked and the identity of the source remains confidential.

The risks of exposure for confidential sources are magnified for female whistleblowers. Therefore, they need to be able to have access to secure digital communications methods to ensure that they are at minimum risk of detection and unmasking. They also need to have confidence in the ability to make secure contact with journalists to ensure that stories affecting women are told – secure digital communications can be an enabler for women’s participation in public interest journalism. They can also help to avoid magnifying the ‘chilling’ of investigative journalism dependent upon female confidential sources. Also needed are strong legal protections for confidentiality, which are applied in a gender-sensitive manner - especially in regard to judicial orders compelling disclosure.”

\section*{Online Harassment}

Harassment, threats and online violence severely restricts the enjoyment that persons have of their rights online, particularly vulnerable and marginalised groups, including women and members of sexual minorities. As described by the Pew Research Center: “In its milder forms, it creates a layer of negativity that people must sift through as they navigate their daily routines

\textsuperscript{91} Id at p 134.
\textsuperscript{92} Id.
\textsuperscript{93} Id.
online. At its most severe, it can compromise users’ privacy, force them to choose when and where to participate online, or even pose a threat to their physical safety."94 Social media platforms are an especially fertile ground for online harassment, but these behaviours occur in a wide range of online venues.95 For those who experience online harassment directly, these encounters can have profound real-world consequences, ranging from mental or emotional stress to reputational damage or even fear for one’s personal safety.96 Furthermore, whether one is affected directly or indirectly by it, it can lead to significant self-censorship to avoid incurring such harassment.

While the internet provides a forum for people to seek information about their identities and sexual orientation, and to express themselves on these topics, many people suffer a wide range of attacks in doing so, including attacks on sexuality, exposing personal information, and the manipulation of images that are then used for blackmail and destroying credibility. Furthermore, a common trend amongst children using the internet involves so-called ‘cyberbullying’. Research has shown that online harassment is often focused on personal or physical characteristics, with political views, gender, physical appearance and race being among the most common.97 Furthermore, women encounter sexualised forms of online harassment at much higher rates than men.98

A particular form of harassment, typically towards women, is that of ‘revenge porn’ online. This relates to a gross violation of a person’s privacy where private and sexually explicit video and photographic images are published, without permission and consent, onto various websites for the purposes of extortion, blackmail and/or humiliation. In South Africa, a proposed legislative amendment seeks to criminalise the distribution of private sexual photographs and films.

Ongoing harassment and attacks on members of the media have become a particularly worrying trend. As stated in the preamble to the 2011 African Commission Resolution on the Safety of Journalists and Media Practitioners in Africa,99 freedom of expression, press freedom and access to information can only be enjoyed when journalists and media practitioners are free from intimidation, pressure and coercion.

**Types of online harassment**


---

95 Id.
96 Id.
97 Id.
98 Id.
• **Cyberbullying**: An umbrella term (like “online harassment”) meant to encompass a number of harassing online behaviours. Like physical bullying, “cyberbullying” is generally aimed at young people and may involve threats, embarrassment, or humiliation in an online setting.

• **Cyber mob attacks**: Cyber-mob attack occurs when a large group gathers online to try to collectively shame, harass, threaten, or discredit a target. Targets overwhelmingly belong to traditionally marginalized groups. “Outrage mobs” or “shaming mobs” are a distinct kind of cyber mob made up of internet users who collectively troll individuals in the hopes of silencing or publicly punishing them. Targets of outrage mobs are often attacked for expressing opinions on politically charged topics or ideas the outrage mob disagrees with and/or has taken out of context in order to promote a particular agenda. Outrage mobbing can sometimes have severe consequences offline and has even resulted in targets losing their jobs.

• **Cyberstalking**: In a legal context, “cyberstalking” is the prolonged use (a “course of conduct”) of online harassment intended to kill, injure, harass, intimidate, or place under surveillance a target. Cyberstalking can comprise a number of harassing behaviours committed repeatedly or with regularity that usually cause a target to suffer fear, anxiety, humiliation, and extreme emotional distress.

• **Denial of service (DoS) or Distributed Denial-of-Service (DDoS) attacks**: A DoS attack is a cyberattack that temporarily or indefinitely disrupts internet service by overwhelming a system with data, resulting in the web server crashing or becoming inoperable. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (such as banking), or other services that rely on the affected computer. In a DDoS attack, an attacker takes control of one user’s computer in order to attack a different user’s computer. This can force the hijacked computer to send large amounts of data to a particular website or send spam to targeted email addresses.

• **Doxing (or doxxing)**: Doxing involves publishing someone’s sensitive personal information online in an attempt to harass, intimidate, extort, stalk, or steal the identity of a target. “Sensitive information” can include social security numbers, phone numbers, home addresses, personal photos, employment information, email addresses, and family members’ personal information.

• **Hateful speech and online threats**: By far the most common form of online harassment, hateful speech or threats, both explicit and implicit, can be issued by an ill-intentioned internet user pretty much anywhere on the web. Hateful speech is a form of expression attacking a specific aspect of a person’s identity, such as one’s race, ethnicity, gender identity, religion, sexual orientation, or disability. Hateful speech online often takes the form of ad hominem attacks, which invoke prejudicial feelings over intellectual arguments in order to avoid discussion of the topic at hand by attacking a person’s character or attributes. Threats issued online can be just as frightening as they are offline, and are frequently meant to be physically or sexually intimidating.
• **Message bombing**: “Message bombing” is the intentional flooding of a person’s or institution’s phone or email accounts with messages meant to limit or block a user’s access to a device’s operating system or platform. Because large numbers of messages sent in a short period of time can typically render a person’s account unusable, this is an effective way for a harasser to prevent you from using your devices or accessing your online accounts. Message bombing typically occurs over texting apps, chat apps, or email accounts.

• **Non-consensual, intimate images and videos (such as “revenge porn”)**: Non-consensual pornography — or revenge porn, as it’s commonly called — is the distribution of private, sexually-explicit images or videos of individuals without their consent. Revenge porn can also fall under the category of “sextortion,” i.e. the threat of distributing a nude or sexually-explicit image or video in an effort to blackmail an individual.

• **Online impersonation**: “Online impersonation” is a strategy whereby harassers create hoax social media accounts, usually in order to post offensive or inflammatory statements in your name. In most cases, the harasser’s intention is to defame or discredit you, often by convincing others to believe the fake quotes attributed to you, which might then incite others to commit additional acts of harassment. Impersonation trolling can also happen when a harasser impersonates someone you know in order to offend or hurt you.

• **Online sexual harassment**: Online sexual harassment – which is targeted at women at a far higher rate than men – encompasses a wide range of sexual misconduct on digital platforms, and includes some of the more specific forms of online harassment, such as “revenge porn”. It often manifests as hateful speech or online threats. There are four distinct types of online sexual harassment: non-consensual sharing of intimate images and videos; exploitation, coercion and threats; sexualised bullying; and unwanted sexualisation.

• **Trolling**: “Trolling” is one of those terms that’s evolved so much over time as to have no single agreed-upon meaning. The term “trolling” is defined here as the repetitive posting of inflammatory or hateful comments online by an individual whose intent is to seek attention, intentionally harm a target, cause trouble and/or controversy, and/or join up with a group of trolls who have already commenced a trolling campaign. There are three subcategories of trolling to be aware of: concern trolling, where harassers pose as fans or supporters of your work with the intention of making harmful or demeaning comments masked as constructive feedback; dogpiling, where a group of trolls works together to overwhelm a target through a barrage of disingenuous questions, threats, slurs, insults, and other tactics meant to shame, silence, discredit, or drive a target offline; and botnet or sock-puppet trolling, which are used for a variety of reasons, from promoting propaganda to amplifying hate or defamation against targeted individuals.
Arguably, one of the key challenges is in getting lawmakers and law enforcement officials to recognise the severity of such harassment and threats, and to treat it with the appropriate levels of concern, recognising that the real and persistent harm suffered applies whether the harassment and threats take place online or offline. Two further challenges that arise that are exacerbated in the online sphere relates to the volume of threats that can be received given the relative ease with which this can be done via social media platforms, for instance; and the concurrent difficulties in identifying perpetrators who are sometimes able to mask their online identities.

This ties in with the issue of anonymity online. This is because one of the particular challenges with online harassment is that perpetrators may mask their identities, making it difficult for law enforcement officials to apprehend them. This, however, should not be seen as a sufficient basis to allow for a blanket ban on anonymity or encryption online. The UNSR on Freedom of Expression has responded to this concern and has stated that:

“The "dark" side of encryption and anonymity is a reflection of the fact that wrongdoing offline takes place online as well. Law enforcement and counter-terrorism officials express concern that terrorists and ordinary criminals use encryption and anonymity to hide their activities, making it difficult for Governments to prevent and conduct investigations into terrorism, the illegal drug trade, organized crime and child pornography, among other government objectives. Harassment and cyberbullying may rely on anonymity as a cowardly mask for discrimination, particularly against members of vulnerable groups. At the same time, however, law enforcement often uses the same tools to ensure their own operational security in undercover operations, while members of vulnerable groups may use the tools to ensure their privacy in the face of harassment. Moreover, Governments have at their disposal a broad set of alternative tools, such as wiretapping, geo-location and tracking, data-mining, traditional physical surveillance and many others, which strengthen contemporary law enforcement and counter-terrorism.”

Where journalists allege imminent threats to their safety, courts are empowered to grant interdictory relief in appropriate circumstances and subject to the relevant legal requirements. For instance, in the matter of *South African National Editors Forum and Others v Black Land First and Others,* the South African high court granted an interdict in favour of the media broadly, in terms of which the respondents were interdicted from “engaging in any of the following acts directed towards the applicants: Intimidation; Harassment; Assaults; Threats; Coming to their homes; or acting in any manner that would constitute an infringement of their personal liberty”, and from “making any threatening or intimidating gestures on social media … that references any violence, harm and threat”.102

---

102 Id. at para 29.
Module 4: Privacy and Security Online

**Protection orders**


Section 4 of the South African Protection from Harassment Act provides that if a court is satisfied that a protection order must be issued as a result of harassment that has taken place over electronic communications or e-mail, and the identity of the respondent is not known, the court may issue a direction to an electronic communications service provider directing that it furnish the court with the following information on affidavit:

- The electronic communications identity number from where the harassing electronic communications or electronic mail originated.
- The name, surname, identity number and address of the respondent to whom the electronic communications identity number has been assigned.
- Any information which indicates that electronic communications or electronic mail were or were not sent from the electronic communications identity number of the respondent to the electronic communications identity number of the complainant.

Any other information that is available to an electronic communications service provider that may be of assistance to the court to identify the respondent or the electronic communications service provider which provides a service to the respondent.

The 2011 ACHPR Resolution noted that killings, attacks and kidnapping of journalists, which are contrary to international humanitarian and human rights law, are often committed in an environment of impunity. As stated in the 2016 UN Resolution on the Safety of Journalists, such impunity constitutes one of the greatest challenges to the safety of journalists, and ensuring accountability for crimes committed against journalists is a key element in preventing future attacks.

Principle XI of the Declaration of Principles on Freedom of Expression in Africa provides as follows:

“**Attacks on media practitioners**

(1) Attacks such as the murder, kidnapping, intimidation of and threats to media practitioners and others exercising their right to freedom of expression, as well as the material destruction of communications facilities, undermines independent journalism, freedom of expression and the free flow of information to the public.

(2) States are under an obligation to take effective measures to prevent such attacks and, when they do occur, to investigate them, to punish perpetrators and to ensure that victims have access to effective remedies.

(3) In times of conflict, States shall respect the status of media practitioners as non-combatants.”
General Comment No. 34 provides that an attack on any person because of the exercise of his or her right to freedom of expression, including forms of attack such as arbitrary arrest, torture, threats to life and killing, cannot be justified under article 19 of the ICCPR.\textsuperscript{103} It states further that journalists, as well as other persons involved in gathering and analysing information about human rights situations such as lawyers and judges, are frequently subjected to threats, intimidation and attacks because of their activities.\textsuperscript{104}

Although it is clear that what is required in the face of online attacks is swift and firm justice, the reality is that many perpetrators commit such with impunity.\textsuperscript{105} Impunity perpetuates a cycle of violence: it raises serious concern that when such attacks go unpunished, this sends a public signal that the state and public authorities do not take such attacks seriously.\textsuperscript{106}

There is therefore clear guidance under international law that states must take measures to protect persons, including members of the media, against such harassment and attacks. This is so whether the harassment takes place offline or online.

**Tips for digital safety to protect against online harassment and trolling**


- Create long and strong passwords for your accounts. (Password managers are useful tools to be able to remember the different passwords used for different accounts.)
- Turn on two-factor authentication.
- Review your privacy settings for each account and make sure any personal data, such as phone numbers and date of birth, is removed.
- Look through your accounts and remove any photos or images that could be manipulated and used as a way to discredit you.
- Consider getting your account verified by the social media company.
- Monitor your accounts for signs of increased trolling activity or for indications that a digital threat could become a physical threat.
- Speak with family and friends about online harassment

\textsuperscript{103} General Comment No. 34 at para 23.
\textsuperscript{104} General Comment No. 34 at para 23.
\textsuperscript{106} Id.