BANWO & IGHODALO

# Legal exceptions to privacy rights in Nigeria: Implications for data subjects and recommended safeguards against arbitrary surveillance

OCTOBER 27, 2025

## Introduction

The right to privacy is widely recognized as a human right, guaranteed under numerous international conventions, and protected in the constitutions and national legislation of many countries around the globe. In Nigeria, the right to privacy is considered a fundamental human right and is enshrined in Chapter IV of the Constitution of the Federal Republic of Nigeria, 1999 (as amended) (the **"Constitution"**).

The right to privacy presupposes that individuals should have freedom to a private life, free from arbitrary intervention from uninvited individuals and state actors. As advancement in technology and innovation continues, leading to the development of new autonomous systems and big data analytics which have transformed data processing, the right to privacy has evolved to include major obligations to protect and manage personal data in the possession of natural and artificial persons. An important corollary of this development is that numerous municipal, national and international legal instruments now contain data protection safeguards against violation of the privacy right of data subjects during data processing activities.

As fundamental and important the right to privacy may seem or may have become, it is not an absolute right. In many jurisdictions, it is acceptable to restrict the right to privacy through surveillance or censorship, particularly when prescribed by law or necessary and proportionate to the achievement of a legitimate endeavor. However, in many instances, the state actors who rely on the legal exceptions to privacy rights often engage in arbitrary intrusions into the private life of citizens beyond the level contemplated by the enabling statutes, thereby resulting in rights abuse.

This article examines the legal framework safeguarding the right to privacy in Nigeria and highlighting instances where restrictions of the rights are lawful and permissible. Implica-

tions of the various legal restrictions are also analyzed within the context of the constitutional guarantee to privacy rights. The article further identifies existing safeguards against arbitrary restrictions and breaches and recommends additional safeguards in line with global best practices.

## Laws allowing breach and restriction to the right to privacy

The Constitution, in section 37, provides for certain conditions for the derogation from some fundamental human rights, including the right to privacy. Further to this, the privacy rights of a data subject in Nigeria may be restricted (a) in the interest of defence, public safety, public order, public morality or public health; or (b) for the purpose of protecting the rights and freedom of other persons. This provides the broad exception to the right to privacy under Nigerian law and remains the basis for the enactment of various legislations imposing one form of restriction or the other on privacy rights in Nigeria. The most popular of such laws and regulations together with their implications on the right to privacy are examined below.

### 1. Nigeria Data Protection Act, 2023

In line with the provision of the Constitution, section 3 of the Nigeria Data Protection Act (**"NDPA"**) expressly provides for certain exemptions to the applicability of the NDPA (and by extension the data protection duties and safeguards contained in it) to data processing activities in Nigeria. Consequently, specific obligations (under Part V of the NDPA) relating to the principles governing data processing and lawful basis for processing of personal data, will not apply to a data controller or data processor if the processing of personal data is -

a. carried out by a competent authority for the purposes of the prevention, investigation, detection, prosecution, or adjudication of a **criminal offence or the execution of a criminal penalty,** in accordance with any applicable law.
b. carried out by a competent authority for the purposes of prevention or control of a **national public health emergency**.
c. carried out by a competent authority, as is necessary for **national security**.
d. in respect of publication in the **public interest**, for **journalism**, **educational**, **artistic** and **literary** purposes to the extent that such obligations and rights are incompatible with such purposes; or
e. necessary for the establishment, exercise, or defense of **legal claims**, whether in court proceedings, or in an administrative or out-of-court procedure

The foregoing clearly indicates a handful of instances where the privacy rights of data subjects are not absolute and may be restricted

### 2. Terrorism (Prevention and Prohibition) Act, 2022

Under section 68 of the Terrorism (Prevention and Prohibition) Act, 2022 (**"Terrorism Act"**), a court on the application of a relevant agency, with the approval of the National Security Advisor, for the purposes of preventing, investigating, and prosecuting terrorism activities, may issue an Interception of Communication Order requiring a communication service provider or law enforcement agency to intercept and retain any specified communication, including call records, data or metadata. The order will specify the period for which a communication service provider may be required to retain communications data to which the order relates.

In addition to this, any information contained in an intercepted communication and retained pursuant to such an order of the court, whether in Nigeria or by a foreign state, is admissible in proceedings for an offence under the Terrorism Act, as evidence of the truth of its content. The Terrosim Act therefore allows for intrusions into the privacy of

individuals when it is necessary to prevent, detect, investigate and prosecute terrorism and other related offences in Nigeria. In this instance, national security serves as the rationale for bypassing the right to privacy of data subjects

### 3. Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 (as amended 2024)

Pursuant to the powers granted under the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 (as amended 2024) (the **"Cybercrimes Act"**), a law enforcement agency may, through its authorized officer, request for the release of any information (traffic data, subscriber information, non-content information and content data) from service providers. Where this occurs, the service provider shall be under a legal obligation to comply. However, the law requires any information obtained to be utilized only for legitimate purposes as prescribed by the Cybercrimes Act or specified in any other relevant legislation or regulation, or by an order of a court of competent jurisdiction. In a similar vein, the Cybercrimes Act empowers Judges to make orders mandating service providers or law enforcement officers to intercept, collect, or record any electronic communication for the purposes of criminal investigations or court proceedings.

### 4. Mutual Assistance in Criminal Matters within the Commonwealth (Enactment and Enforcement) Act, 2019

The Act gives legal force in Nigeria to the Commonwealth's legal instrument for mutual assistance in criminal matters. It allows Nigeria to cooperate with other Commonwealth countries in providing assistance through the exchange of information relating to persons and entities for the purposes of criminal investigation.

The assistance that may be exchanged under the Act between Nigeria and a foreign State include activities that involve processing of the personal data of relevant data subject (without compliance with data protection safeguards such as obtaining consent or cross-border transfer controls). Such assistance include: (a) identifying and locating criminal offenders; (b) the service of relevant documents; (c) examination of witnesses; (d) search and seizure of assets; (e) obtaining evidence; (f) facilitating the personal appearance of witnesses before an administrative panel, a court, a tribunal or such similar proceedings; (g) effecting a temporary transfer of a person in custody to enable him appear as a witness; (h) securing the production of official or judicial records; and (i) tracing, seizing and forfeiting the proceeds of criminal activities.

### 5. Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries, 2022

The Code of Practice was issued by the National Information Technology Development Agency (NITDA) in 2022. It applies to all Interactive Computer Service Platforms/ Internet Intermediaries, including entities that are their subsidiaries, affiliates, and agents in Nigeria. The Code places an obligation on these platforms and intermediaries to, upon the order of a court of competent jurisdiction, disclose the identity of the creator of any information and provide any information under their domain to any authorized government agency. Such order may be made for, among other purposes, the prevention, detection, investigation, or prosecution of an offence concerning the sovereignty and integrity of Nigeria, public order, security, diplomatic relationships, felony, incitement of an offence relating to any of the above or in relation to rape, child sexual abuse or cybercrimes.

### 6. Lawful Interception of Communications Regulations, 2019

The Lawful Interception of Communications Regulations were issued by the Nigerian Communications Commission (NCC) and is considered the most comprehensive law on communication surveillance in Nigeria. The Regulations

provide a framework for lawful interception of communication, collection and disclosure of intercepted communications in Nigeria. Further to this, it is lawful for any authorized agency listed in the Regulations to intercept any communication, or to do so pursuant to any legislation in force via a warrant:

a) in the interest of national security
b) for the purpose of preventing or investigating a crime
c) to protect and safeguard the economic well-being of Nigerians
d) in the interest of public emergency or safety
e) towards giving effect to any international mutual assistance agreements to which Nigeria is a party.

It should be noted that, there are instances where an authorized agency can intercept communication without a warrant, such as where: (a) there is immediate danger of death or serious injury to any person; (b) there exists activities that threaten the national security; or (c) activities having characteristics of organized crime are involved. However, the relevant authorized agency must apply for a warrant within 48 hours after the interception has been carried out. Where the required application is not made or is denied, the interception shall terminate immediately, and further interception shall be unlawful. Generally, a warrant is granted for a maximum period of three (3) months and renewable for another maximum period of three (3) months.

## Existing safeguards for the right to privacy

While the right to privacy may not be absolute, it is necessary to ensure that the permissible restrictions under the law are justified and legitimate, aligning with the provisions of the Constitution. A review of the laws and regulations discussed above indicates a critical safeguard in the legal framework for the restrictions of privacy rights in Nigeria – the Judiciary. The judiciary lies at the heart of protecting the right to privacy and is tasked with the critical responsibility of ensuring that the prescribed conditions for intrusion into the privacy of data subjects are met by state actors, through the duty to authorize such intrusion by issuing warrants/orders. A few of the instances where the judiciary is required to play such role are discussed below.

- **Section 58 of the NDPA** requires the Nigeria Data Protection Commission to apply *ex-parte* to a Judge in Chambers for the issuance of a warrant to obtain evidence in relation to an investigation. However, the issuance of the warrant is conditioned upon the Judge's satisfaction that (i) a person has engaged, is engaging, or is likely to engage in a conduct that contravenes the law; (ii) the warrant is sought to prevent the commission of an offence under the NDPA; (iii) the warrant is sought to prevent interference with investigative process under the law; (iv) the warrant is sought for the purpose of investigating data security breaches and data privacy breaches, or obtaining electronic evidence; or (v) the person named in the warrant is preparing to commit an offence under the NDPA.

- **Section 39 of the Cybercrimes Act** imposes an obligation on authorized agencies, even where there are reasonable grounds to suspect that the content of any electronic communication is necessary for the purposes of criminal investigations or proceedings, to obtain an order either compelling a service provider to deploy technical means to intercept, collect, record, permit or assist competent authorities with the collection or recording of information associated with specified communications transmitted by means of a computer system; or authorising a law enforcement officer to collect or record such information through application of technical means. A Judge may grant the foregoing order only on the basis of information on oath, implying the exercise of discretion which must be judicious and judicial.

- **Section 45(3) of the Cybercrimes Act** contains similar provisions to the NDPA and requires that before a court issues a warrant to the relevant authorities, it must be satisfied that the warrant is sought to prevent the commission of an offence under the Cybercrimes Act, or for investigative purposes or prevention of interference with investigative process connected with cybercrimes or related offences.

- **Regulation 7 of the Lawful Interception of Communications Regulations** similarly illustrates the discretion of the court in granting a warrant for the interception of communication. Accordingly, a Judge may not issue a warrant unless the warrant is necessary, and such information can only be obtained by the lawful interception of the communication. The regulation further provides that a warrant is necessary where it is in the interest of national security, for preventing a crime, for the purpose of public emergency, or for giving any international mutual assistance

Other safeguards introduced by law include the imposition of time limitation of duration of the restriction of privacy rights of data subjects. For instance, *Regulation 6 of the Lawful Interception of Communications Regulations* requires that the intercepted communication received by the relevant authority must be destroyed upon the completion of such investigation and any non-relevant information obtained in the course of the interception must be destroyed upon extraction of the relevant portion of such communication. Also, other copies of any intercepted communication admitted in evidence by a court of competent jurisdiction must be destroyed. The Regulation allows a retention period of three (3) years during which an agency can retain any intercepted communication in its custody.

Additional safeguards include the requirement to keep such retained information confidential, to be shared only for the purpose of investigation and prosecution in criminal proceedings in accordance with the Regulations (Regulation 6 of the Lawful Interception of Communications Regulations). An additional layer of scrutiny is also introduced with the requirement in *Regulation 19 of the Lawful Interception of Communications Regulations* that every authorized agency should prepare a report on all concluded interception cases carried out annually and submit the report to the Attorney-General.

## Developing effective safeguards for the right to privacy

Regardless of the various rationale for intrusion, surveillance and restriction on the right to privacy, it is important to ensure that the derogation from the right is fair and judicious, to prevent abuse of power by authorised agencies. Where any law or regulation leaves loopholes for arbitrariness, impunity, and illegality on the part of authorized government and/or private agents, it is recommended that such law or regulation should be amended to enshrine international guiding principles of privacy rights. In order to strike a healthy balance between the protection of public interests and the protection of the individual's right to privacy, we propose the following guiding principles for legislative reform:

- **Necessity and proportionality**: It is vital to determine the propriety of communications surveillance, to consider whether such surveillance is necessary to achieve a legitimate aim, and whether the intrusion into the right to privacy is proportionate to the aim sought to be achieved. As such, our laws should restrict broad discretion of security agencies and state actors to seek or order surveillance measures.

- **User notification**: International human rights standards require, as a rule, that every subject of communications surveillance be notified of the decision authorizing surveillance, unless such notification will seriously jeopardize the purposes of the surveillance. However, there is no provision for user notification, either during or after a surveillance exercise, in our extant laws. In most cases, applications for court orders or warrants are generally *ex-parte*, meaning that the subjects/ targets of court orders are typically not put on notice. Failure to notify data subjects of pending applications against them in court means they cannot promptly challenge the breach of their rights or seek remedy for such breaches, where such breaches are considered unlawful. It is therefore critical to incorporate user notification provisions in our legal framework, especially in circumstances where user notification will not impede the purposes for surveillance.

- **Transparency and oversight:** It is equally an international human rights standard to require state actors to prioritize transparency in decisions regarding communications surveillance. This will involve publishing reports detailing aggregate information on surveillance authorizations and maintaining public oversight through an independent monitoring system that can hold the authorities accountable. However, there is no current oversight mechanism in our extant laws that mandate transparency and oversight mechanisms. Developing a robust checks and balances system is critical to ensuring that security agencies engage in communications surveillance only for legitimate reasons

## Conclusion

The debate on the right to privacy in Nigeria seems polarized between maintaining the collective public interest and safety and safeguarding the individual fundamental right to privacy and dignity of the human person. The solution undoubtedly lies in a balancing act between the guaranteed right to privacy and the welfare of others, the investigation of criminal activities, the prevention of crime and curbing cyberattacks.

While the current framework of laws and regulations have substantially provided for judicial safeguards against arbitrary intrusions into the private life of citizens, additional guidance and oversight are desired. The applicable laws are largely yet to fully conform with internationally accepted principles and policies guiding surveillance practices. Notably, transparency, effective independent oversight, and user notification are necessary for the current Nigerian surveillance framework. It is important to ensure our laws reflect these principles and incorporate them as a cornerstone of our surveillance activities. This will guarantee that the right to privacy is protected in accordance with international human rights standards while efficiently balancing public interest and national security concerns.



## CONTACT PERSONS

**Olumide Osundolire**

Partner

E: Oosundolire@banwoighodalo.com

**Ada Aguocha**

Senior Associate

E: Aaguocha@banwoighodalo.com

**Vanessa Obi**

Associate

E: VObi@banwo-ighodalo.com

**Oluwatoba Oguntuase**

Senior Support Lawyer

E: ooguntuase@banwo-ighodalo.com