# The Right to Privacy in the Digital Age

About Tech Hive™

Tech Hive Advisory Limited ("Tech Hive") is a technology policy advisory and research firm that provides support to private and public organisations concerning the intersection of technology, business, and law. We focus on how emerging and disruptive technologies alter and influence the traditional way of doing things while acting as an innovation partner to our clients.

Our experience and capability extend across Research and Policy Advisory, Privacy and Data Protection, Data Ethics, Cybersecurity, Start-Up Advisory, and Digital Health. We ensure our advice serves our clients well by understanding their business and the markets they operate in through accurate policy and legislative development tracking and intelligence.

**Contact:** contact@techhiveadvisory.org.ng

**Contributors**

Akintunde Agunbiade
Oghosa Eghe-Abe
Ogundele Tolulope
Oluwagbeminiyi Ojedokun
Ridwan Oloyede
Sandra Musa

**Introduction**

In this contribution, Tech Hive Advisory focuses on four manifestations and related infractions of the right to privacy in the digital age-related to Nigeria. These are:

- Targeted and mass surveillance, including of journalists and human rights defenders;
- Digital identity systems rolled out by the Nigerian government and companies operating in Nigeria;
- Use of biometrics for identification and authentication;
- Covid-19 response; and
- Use of encryption and anonymity technologies.

This contribution primarily aggregates our previous research in the past five years regarding the right to privacy whilst providing updated insights for tackling the issues raised.

**Issue**

*Targeted and mass surveillance, including journalists and human rights defenders.*

**Comments**

Despite the government's obligation to protect the right to privacy under most Constitutions, threats to this right have increased. One of the forms of this threat is State-ordered mass surveillance carried out by the government against its critics, including journalists[1] and human rights defenders, with the backing of intrusive digital technologies and faulty laws.

We have seen increased budgetary allocations for procurement of surveillance tools, enacting new laws or amending existing laws to increase government surveillance powers[2] and arbitrary surveillance deployment. In addition, there are examples of government monitoring social media use,[3] arbitrary arrest and conviction of journalists or government critics[4], and state actors acting outside what is legally permissible. For example,

[1] For instance, in Nigeria, the government has relied on Section 24 of the Cybercrimes Act to arrest several journalists arbitrarily. As a result, the provision has been criticised by the Court of Justice of the Economic Community of West African States as excessive and contrary to established international norms and conventions on human rights. COURT ORDERS NIGERIA to ALIGN ITS CYBERCRIME LAW with ITS INTERNATIONAL OBLIGATIONS' (*Courtecowas.org*2015) <http://www.courtecowas.org/2022/03/27/court-orders-nigeria-to-align-its-cybercrime-law-with-its-international-obligations/#:~:text=The%20ECOWAS%20Court%20of%20Justice,International%20Covenant%20on%20Civil%20and> accessed 4 June 2022

[2] In Nigeria, the 2021 *Draft Registration of Telephone Subscribers Regulation* also retains the provision in the 2011 Regulation that allows the telecoms regulator, the Nigerian Communications Commission (NCC), to disclose subscribers' information to security agencies without recourse to the law courts.

[3] 'Government Social Media Spying Powers: 50 Countries Ranked on Social Media Surveillance - Comparitech' (*Comparitech.com*2018) <https://www.comparitech.com/blog/vpn-privacy/gov-social-media-surveillance/> accessed 4 June 2022

[4] YEKEEN Akinwale, 'Violation of Court Orders, Arrest of Journalists, Other Anti-Democratic Actions of Buhari Administration' (*International Centre for Investigative Reporting*6 August 2019) <https://www.icirnigeria.org/violation-of-court-orders-arrest-of-journalists-other-anti-democratic-actions-of-buhari-administration/> accessed 4 June 2022

a 2021 report on the State of surveillance in six African countries finds that the six African countries examined lack a sufficient legal framework for communications surveillance to guarantee human rights.[5]

In addition, the lack of strong accountability in the global surveillance tools market makes it easy to acquire these tools by repressive governments and state agents, who use these tools to monitor and profile citizens, critics, journalists and human rights advocates[6]. The promises made by these companies are not enough[7] to safeguard human rights. For example, the NSO group spyware, Pegasus, has been reportedly used to monitor world leaders in 34 countries.[8]

**Recommendations**

- Laws enabling surveillance and suppression of freedom of expression should be reviewed for vague terms like 'inconvenience', 'annoyance', or 'insult', which leaves room for indiscriminate interpretation and is used for censorship and suppression of journalists and human rights defenders. Also, an amendment should be made to the law to comply with international human rights standards.
- Laws enabling surveillance should provide additional safeguards as recommended under the African Commission (2019) Declaration of Principles on Freedom of Expression and Access to Information, International Principles on the Application of Human Rights to Communications Surveillance, the United Nations Draft Legal Instrument on Government-led Surveillance and Privacy, and other international instruments to entrench human rights protection. For example, there should be a consideration for human rights impact assessment before surveillance tools are deployed, surveillance should be anchored on law, there should be transparency, it should allow notification and room for appeal, it must be necessary and proportionate, there should be an independent judiciary and an independent oversight body, among others.
- There should be strong accountability measures, possibly a global action against State and non-state actors using these repressive Spywares. They should be held responsible.
- There should be a global action against abuse and arbitrary surveillance of journalists.
- Member states must ensure that surveillance is used for the most severe crimes, grounded in law, and the law must conform with established human rights norms

**Issue**

*Digital identity systems, use of biometrics for identification and authentication.*

---

[5] Roberts, T.; Mohamed Ali, A.; Farahat, M.; Oloyede, R. and Mutung'u, G. (2021) Surveillance Law in Africa: a review of six countries, Brighton: Institute of Development Studies, DOI: 10.19088/IDS.2021.059

[6] Pegasus: Spyware Sold to Governments "Targets Activists (*BBC News*19 July 2021) <https://www.bbc.com/news/technology-57881364> accessed 4 June 2022

[7] Israel Envoy Says Firms like Pegasus-Maker NSO Can't Sell to Non-Government Actors' (*Republic World*28 October 2021) <https://www.republicworld.com/world-news/rest-of-the-world-news/israel-envoy-says-firms-like-pegasus-maker-nso-cant-sell-to-non-government-actors.html> accessed 4 June 2022

[8] Craig Timberg and others, 'On the List: Ten Prime Ministers, Three Presidents and a King' (*Washington Post*20 July 2021) <https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/> accessed 4 June 2022

The different governments and companies are rolling out digital identity systems and programs. These measures are strengthened by different motivations from identification, immigration, and age appropriation.

**Comments**

The use of digital identity systems can bring about several privacy concerns and affect the privacy rights of individuals in various ways. As a result, more governments have taken steps to roll out digital identity systems to promote effective governance, economic development, and others in the past few years.

In addition to the roll-out of digital identity programs, there is also the trend of government mandating SIM registration and linkage to identity programs. For example, in Nigeria, the government ordered the mandatory linkage of SIM registration to the national identity system[9] and disconnected SIM cards that were not connected. Another noticeable trend is the push for mandatory SIM registration and digitisation of the national identity system in the absence of an adequate data protection law or independent data protection authority.

These measures are being met with some resistance as individuals are concerned with the country's lack of efficient data protection practices, which leaves the data collected open to abuse[10]. Failure to put privacy-preserving measures early on will exacerbate the risk as the national database grows. Some governments are also confronted with creating multiple identity databases maintained by government agencies. These duplicities often lack effective oversight and accountability mechanisms.

Also, there are concerns about state authorities' arbitrary access to the national identity database for surveillance. For example, in Nigeria, the President authorised some law enforcement agencies to access identity databases through mere executive pronouncement when the surveillance should only be hinged on existing law[11].

**Recommendations**

- The use of privacy-preserving tools to ensure that the government only collects personal data that is relevant, necessary and proportionate to the purpose it is required. This includes adopting a privacy by design and default mechanism into the lifecycle of every product/service employed to achieve the government's aim concerning digital identity systems. In addition, employing technical and organisational measures to ensure data security would also be a way to go.

---

[9] NIN-SIM Linkage: Federal Government Commends Compliance and Directs Telcos to Bar Outgoing Calls on Unlinked Lines from 4th April, 2022' <https://www.ncc.gov.ng/media-centre/news-headlines/1191-press-release-nin-sim-linkage-federal-government-commends-compliance-and-directs-telcos-to-bar-outgoing-calls-on-unlinked-lines-from-4th-april-2022> accessed 4 June 2022

[10] Thomson Reuters Foundation, 'Why Millions of Africans Are Right to Resist SIM Card Registration <https://news.trust.org/item/20220503084813-z74ni/> accessed May 30, 2022

[11] NIN-SIM Linkage: Security Agencies Get Buhari's Nod to Access Subscribers' Details." *Punch New spapers*, 4 Feb. 2022, <https://punchng.com/nin-sim-linkage-security-agencies-get-buharis-nod-to-access-subscribers-details/> accessed May 30, 2022.

- There is a need to ensure that data protection authorities are independent and well-resourced to carry out their function.
- Countries digitising identity systems should enact a data protection law and establish an independent authority to enforce the law.
- Non-state players in the digital identity ecosystem should be held to high human rights standards, data protection, and security.
- There is a need for a more important call to legitimise mandatory SIM registration and the mandatory linkage to national identity systems.
- The national identity database should have adequate privacy safeguards implemented and effectively enforced across all agencies and actors in the ecosystem.

**Issue**

Use of encryption and anonymity technologies

**Comments**

Increasing legislative proposals and laws are calling for the weakening or breaking of encryption and eliminating anonymity online. Also, the weakening or creating a backdoor to encryption creates risk and will harm privacy rights, as the access can be abused.[12] For example, the proposed Online Safety Bill in the United Kingdom could weaken the protection provided by encryption.[13] Furthermore, in 2020, "the governments of the U.S., U.K., Australia, New Zealand, Canada, India and Japan have issued the joint statement which pleads with Facebook specifically, as well as other tech firms, to drop "end-to-end encryption." [14] Also, governments acquire surveillance tools capable of breaking encryption. For example, in Nigeria, in July 2021, the Senate approved a budgetary allocation to purchase WhatsApp and Thuraya Interception Solution. Their active deployment poses a threat to end-to-end encryption and the overall right to privacy.[15]

[12] 'Global Encryption Day: Any Backdoor Would Do More Harm than Good.' (*Tutanota*2021) <https://tutanota.com/blog/posts/why-a-backdoor-is-a-security-risk/> accessed 4 June 2022.

[13] 'UK Online Safety Bill Set to Weaken Encryption and Put UK Internet Users at Risk - Internet Society' (*Internet Society*19 January 2022) <https://www.internetsociety.org/blog/2022/01/uk-online-safety-bill-set-to-weaken-encryption-and-put-uk-internet-users-at-risk/#:~:text=19%20January%202022-,UK%20Online%20Safety%20Bill%20Set%20to%20Weaken%20Encryption,UK%20Internet%20Users%20At%20Risk&text=The%20Internet%20Society%20joins%20the,role%20in%20protecting%20users%20online.> accessed 4 June 2022.

[14] Barry Collins, 'Mission Impossible: 7 Countries Tell Facebook to Break Encryption' *Forbes* (11 October 2020) <https://www.forbes.com/sites/barrycollins/2020/10/11/mission-impossible-7-countries-tell-facebook-to-break-encryption/?sh=c477f853a5a3> accessed 4 June 2022.

[15] Ilori, T., Modise, S., Mwanzia S.W., Ayalew, Y.E., Oloyede, R., Musa, O.S., Borokini, F., 'The intersection of the right to freedom of expression online and protection of personal information in Botswana, Ethiopia, Kenya, and Nigeria' (Tech Hive Advisory, September 2021) https://techhiveadvisory.org.ng/new-report/ accessed May 30 2022, p. 78

Anonymity is required by journalists, dissidents, vulnerable populations, human rights advocates, and others to protect their identities. The increased call for a ban on anonymity by government[16] and private actors[17] will deny people who need anonymity the protection they require. Both anonymity and encryption are needed to protect the right to privacy and freedom of expression online. For example, the newly introduced Cybercrimes Act in Syria suppresses anonymity and imposes an obligation on service providers.[18]

Besides Article 17 of the ICCPR, Principle 40 of the *African Declaration of Principles on Freedom of Expression and Access to Information in Africa*[19] requires States to guarantee the right to privacy, the confidentiality of communication and the protection of personal information within their respective jurisdictions. Accordingly, states must preserve the right to privacy through anonymity, preservation of encryption and safeguard against illegitimate third-party intrusion into private communications. State parties are also prohibited from adopting measures that weaken the security architecture needed to preserve digital communications privacy.

Ensuring the privacy of digital communications is where encryption becomes necessary. The UN Rapporteur noted that encryption and anonymity enable private communications and shield an opinion from outside scrutiny, critical in hostile political, social, religious and legal environments.[20]

**Recommendations**

- There is a need for member states to increase the call to preserve encryption and anonymity. But, conversely, calls to weaken or break encryption should be resisted.
- Laws enabling the weakening of encryption should be reviewed to ensure law enforcement agencies cannot mandate the decryption of encrypted information without judicial review.[21]
- Recent calls and legislative proposals to erode anonymity should be dismissed, and anonymity should be maintained to protect vulnerable populations, human rights advocates, dissidents and other stakeholders.

**Issue**

[16] Lee Rainie, Janna Anderson and Jonathan Albright, 'The Future of Free Speech, Trolls, Anonymity and Fake News Online' (*Pew Research Center: Internet, Science & Tech*29 March 2017) <https://www.pewresearch.org/internet/2017/03/29/the-future-of-free-speech-trolls-anonymity-and-fake-news-online/> accessed 4 June 2022.
[17] Cristiano Lima and Aaron Schaffer, 'Elon Musk Wants to "Defeat the Spam Bots" but Faces a Free Speech Problem' (*Washington Post*27 April 2022) <https://www.washingtonpost.com/politics/2022/04/27/elon-musks-plan-defeat-spam-bots-has-free-speech-problem/> accessed 4 June 2022.
[18] 'Syria's New "Cybercrime" Law Adds Salt to Injury - Access Now' (*Access Now*27 May 2022) <https://www.accessnow.org/syria-cybercrime-law/> accessed 4 June 2022.
[19] ACHPR, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (2019) https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf accessed May 30 2022
[20] Ibid para. 12
[21] Ibid, pp. 88 - 89

*Measures relying on digital technology taken to combat the Covid-19 pandemic.*

**Comments**

Following the outbreak of the Covid-19 pandemic, several governments and private organisations sought to leverage technology to curb the spread of the pandemic. Solutions were introduced for self-triaging, warning the public and contact tracing. However, in the early days of the pandemic, there were debates if decentralised or centralised solutions offered privacy, and different governments adopted different solutions. In addition, the government had a different regulatory response. Different data protection authorities published guides, guidelines, and deliberations on data protection measures that should be adopted. However, the period also recorded government abuse of a public health epidemic to abuse, collect excess data and violate privacy rights[22].

In Nigeria, a few sub-national governments introduced mobile applications for self-triaging. One of them was Kogi State, which introduced a Covid-19 app, available via http://www.kogicovid19.com.ng/. The mobile application[23] was hosted as a third party application that is not unavailable on any recognised app store. The application did not have an SSL (Secure Socket Layer) certificate, there was no privacy notice, and the app was collecting information that was not necessary for self-triaging. While the Kogi Covid-19 app may be well-intentioned, it fails to safeguard privacy rights and data processing principles for managing health data.

**Recommendations**

- Data protection impact assessment should be conducted before deploying the technological solution to combat a public health disaster.
- Data processing principles like security, data minimisation, transparency, and fairness should be embedded into the solution development.
- Data protection by design and default and security should be embedded throughout the lifecycle of solutions, projects and products to respond to public health crises.
- Data collected during these periods should not be held longer than necessary.

[22] Dyani Lewis, 'Why Many Countries Failed at COVID Contact-Tracing — but Some Got It Right' (2020) 588 Nature 384 <https://www.nature.com/articles/d41586-020-03518-4> accessed 4 June 2022.

[23] Odeshina, N., Oloyede, R., 'Assessment of Government COVID-19 Mobile Applications (Apps) in Nigeria', (Tech Hive Advisory, May 2020) https://techhiveadvisory.org.ng/assessment-of-government-covid-19-mobile-applications-in-nigeria/ accessed May 30 2022