PRIVACY INTERNATIONAL

Stakeholder Report
Universal Periodic Review
31st Session - Nigeria

The Right to Privacy in Nigeria

Submitted by Paradigm Initiative and Privacy International

March 2018

The Right to Privacy in Nigeria

March 2018

PRIVACY INTERNATIONAL

www.privacyinternational.org

PARADIGM INITIATIVE

INTRODUCTION

1. This Universal Periodic Review ("UPR") stakeholder report is a submission by Privacy International and Paradigm Initiative.[1]

    - Privacy International is a human rights organisation that works to advance and promote the right to privacy around the world. We investigate the secret world of government surveillance and expose the companies enabling it. We litigate to ensure that surveillance is consistent with the rule of law. We advocate for strong national, regional, and international laws that protect privacy. We conduct research to catalyse policy change. We raise awareness about technologies and laws that place privacy at risk, to ensure that the public is informed and engaged.
    - Paradigm Initiative is a non-profit, formed in 2008, that works for the improved livelihoods of underserved youth across Africa through building an information and communications technology ("ICT")-enabled environment and advocating for digital rights. Although Paradigm Initiative—formerly "Paradigm Initiative Nigeria"—originally focused on ICT and digital rights in Nigeria, in recent years it has expanded its mandate to cover the African continent at large.

2. Together Privacy International and Paradigm Initiative wish to bring their concerns about the protection and promotion of the right to privacy in Nigeria before the Human Rights Council for consideration in Nigeria's upcoming review. This stakeholder report highlights four areas of concern:

    - The Nigerian state appears to have significant surveillance capabilities, but the legislation governing communications surveillance fails to abide by international human rights standards.
    - Increased monitoring of online activity by government actors creates an atmosphere of fear around controversial online speech, and may endanger the right to privacy.
    - The absence of comprehensive overarching data protection legislation and the lack of a central independent agency charged with ensuring respect for data protection principles fail to meet international standards and put privacy at risk, particularly in light of concerns around the management of existing government databases and an ongoing database harmonisation scheme.
    - Mandatory registration of all SIM cards, the establishment of a database containing information about users of mobile phone services, and mandatory data retention requirements on internet service providers are measures that contravene international human rights standards on the right to privacy because they are neither necessary to achieve a legitimate aim nor proportionate to the aim pursued.

3. In its resolution on the right to privacy in the digital age, adopted on 23

[1] Privacy International and Paradigm Initiative would like to thank the International Human Rights Clinic at Harvard Law School for its support in the research, preparation, and drafting of this submission.

March 2017, the United Nations Human Rights Council called on all states "to 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."[2] The UPR offers a significant opportunity for states to demonstrate that they are implementing this recommendation, by systematically reviewing states' compliance with their obligations to respect and protect the right to privacy. In the first and second UPR cycles, there was no mention of the right to privacy in Nigeria's National Reports or the Working Group reports.[3]

The Right to Privacy

4. Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[4] It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information, and association. The right to privacy embodies the presumption that individuals should have an area of autonomous development, interaction, and liberty, a "private sphere" with or without interaction with others, free from arbitrary state intervention and from excessive unsolicited intervention by other uninvited individuals.[5] Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[6]

2 "The right to privacy in the digital age," UN Human Rights Council Resolution, A/HRC/RES/34/7 (23 March 2017). See also: "The right to privacy in the digital age," UN General Assembly Resolution, A/C.3/71/L.39 (31 October 2016), "The right to privacy in the digital age," UN General Assembly Resolution, A/RES/69/166 (18 December 2014). The same language appears in a similar resolution passed in the 2013 General Assembly session: "The right to privacy in the digital age," UN General Assembly Resolution, A/RES/68/167 (18 December 2013).

3 National report submitted in accordance with paragraph 15 (a) of the annex to Human Rights Council resolution 5/1, Nigeria, 2009, A/HRC/WG.6/4/NGA/1; Report of the Working Group on the Universal Periodic Review, Nigeria, October 2009, A/HRC/11/26. In particular, members of the Working Group (France, Canada) raised concerns regarding respect for journalists' freedom of expression, especially in the context of government criticism. National report submitted in accordance with paragraph 5 of the annex to Human Rights Council resolution 16/21, Nigeria, 2013, A/HRC/WG.6/17/NGA/1; Report of the Working Group on the Universal Periodic Review, Nigeria, December 2013, A/HRC/25/6. The National Report referenced the enactment of the Terrorism Prevention Act 2011 and its subsequent amendment in 2013; Nigeria's constitutional and statutory guarantees of the rights to freedom of expression and the press; and its work to implement the related recommendation from the first cycle of review. Members of the working group encouraged further promotion of freedom of expression (Estonia), assembly (Estonia), and association (Estonia, United States).

4 Universal Declaration of Human Rights, art 12; United Nations Convention on Migrant Workers, art 14; Convention on the Rights of the Child, art 16; International Covenant on Civil and Political Rights, art 17; African Charter on the Rights and Welfare of the Child, art 10; American Convention on Human Rights, art 11; African Union Principles on Freedom of Expression, art 4; American Declaration of the Rights and Duties of Man, art 5; Arab Charter on Human Rights, art 21; European Convention for the Protection of Human Rights and Fundamental Freedoms, art 8; Johannesburg Principles on National Security, Free Expression and Access to Information; Camden Principles on Freedom of Expression and Equality.

5 Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 2009, A/HRC/17/34.

6 See Universal Declaration of Human Rights, art 29; Human Rights Committee, General Comment No. 27: Article 12 (Freedom of Movement), 2 November 1999, CCPR/C/21/Rev.1/Add.9; Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988.

5. As innovations in information technology have enabled previously unimagined forms of collecting, storing, and sharing personal data, the right to privacy has evolved to encapsulate state obligations related to the protection of personal data.[7] A number of international instruments enshrine data protection principles, and many domestic legislatures have incorporated such principles into national law.[8]

Domestic Law on Privacy

6. The 1999 Constitution of the Federal Republic of Nigeria ("Constitution") recognises privacy as a fundamental right. Section IV, Article 37 of the Constitution provides that "[t]he privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected." However, commentators have described Article 37 as "probably one of the most under-researched, under-litigated and under-developed rights in the Nigerian Constitution."[9]

7. Despite the express guarantee of privacy in the Constitution, Nigeria does not have overarching legislation devoted to the protection of personal information, although, as of March 2018, the National Assembly is considering two bills on the topic. Rules concerning data protection mainly consist of discrete provisions found in agency-specific laws (such as the National Identity Management Commission Act 2007, which governs the country's identity management system) and industry-specific regulations. In 2013, the National Information Technology Development Agency ("NITDA") prepared Draft Guidelines on Data Protection, which contain a detailed set of provisions regulating the collection, processing, storage, and transfer of personal information by government actors.[10] However, the guidelines are not yet binding.[11]

[7] Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy).

[8] See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data; Guidelines for the regulation of computerized personal data files (UN General Assembly Resolution 45/95 and E/CN.4/1990/72). As of January 2018, over 100 countries had enacted data protection legislation and around 40 countries had pending bills or initiatives in the area: David Banisar, "National Comprehensive Data Protection/ Privacy Laws and Bills 2018," 25 January 2018, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416.

[9] Aaron Olaniyi Salau, "Data Protection in an Emerging Digital Economy: The Case of Nigerian Communications Commission: Regulation without Predictability?", 7th International Conference on Information Law and Ethics, 22-23 February 2016, available at http://icil.gr/download.php?fen=years/2016/downloads/documents/icil_2016_proceedings_book.pdf.

[10] See David Oluranti, "Data and Privacy Laws in Nigeria," Nigerian Law Today, 2017, available at http://nigerianlawtoday.com/data-privacy-laws-nigeria/.

[11] "Nigerians alerted on new EU's data protection guidelines," New Telegraph, 22 February 2018, available at https://newtelegraphonline.com/2018/02/nigerians-alerted-new-eus-data-protection-guidelines/.

AREAS OF CONCERN

I. Surveillance Law and Practices

Current Legislation Governing Communications Surveillance

8. There are two pieces of legislation authorising communications surveillance in Nigeria: the Terrorism (Prevention) Act 2011 and the Cybercrimes (Prohibition, Prevention, Etc) Act 2015. Despite incorporating some safeguards, both Acts contain insufficient protections for the right to privacy, as they do not comply with the internationally recognised principles that surveillance policies and practices must observe. These include: legality, necessity, proportionality, judicial authorisation, effective independent oversight, transparency, and user notification, among others.[12]

9. Under the Terrorism (Prevention) Act 2011, law enforcement agencies—with the approval of the Attorney General and the Coordinator on National Security—may apply to a judge for an "interception of communication order" for the purpose of preventing a terrorist act or prosecuting offenders under the Act.[13] Orders can differ significantly in scope. They can: require a communication service provider to intercept and retain specified communications (subject to a maximum retention period, specified by the judge);[14] authorise law enforcement actors to enter any premises to install any device for the interception and retention of communications (it is unclear whether this provision permits remote access to devices);[15] or authorise the law enforcement actors to execute "covert operations" for gathering intelligence in relation to specific terrorist groups or persons.[16]

10. The Act empowers law enforcement agencies to gather intelligence and investigate the offences proscribed under the Act.[17] "Law enforcement agency" is defined to include a large number of law enforcement and security agencies, ranging from the Nigeria Police Force to the Economic and Financial Crimes Commission.[18] The Department of State Security Services ("DSS"), Nigeria's

12 For more information, see International Principles on the Application of Human Rights to Communications Surveillance, a set of principles developed by a range of civil society groups, as well as industry and international experts in communications surveillance law, policy, and technology. These principles "provide civil society groups, industry, States, and others with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights." See "The Principles," International Principles on the Application of Human Rights to Communications Surveillance; Privacy International, Guide to International Law and Surveillance, 2017, available at https://privacyinternational.org/feature/993/guide-international-law-and-surveillance.

13 Terrorism (Prevention) Act 2011 (as amended by the Terrorism (Prevention) Amendment Act 2013), s 29(1).

14 Ibid, s 29(2)(a).

15 Ibid, s 29(2)(b).

16 Ibid, s 29(2)(c).

17 Ibid, s 1(a)(3).

18 The full list of agencies included in the definition of "law enforcement agency" is as follows: Nigeria Police Force; Department of State Security Services; Economic and Financial Crimes Commission; National Agency for the Prohibition of Traffic in Persons; National Drug Law Enforcement Agency; National Intelligence Agency; Nigeria Customs Service; Nigeria Immigration Service; Defence Intelligence Agency; Nigeria Security and Civil Defence Corps; Nigeria Armed Forces; Nigeria Prisons Service; and "any other agency empowered by an Act of the National Assembly." The majority of this list is contained within Section 40 of the Terrorism Prevention Act 2011; Section 40 is augmented by Section 19 of the Terrorism Prevention (Amendment) Act 2013.

primary domestic intelligence agency, is also covered by the Act's definition of law enforcement agency, but there are serious concerns about its surveillance practices, and more broadly, its respect for human rights standards.[19] Additionally, the definition includes the Special Anti-Robbery Squad ("SARS"), a prominent unit of the Nigeria Police Force that has been subject to specific international criticism for its human rights record. Amnesty International has noted that SARS has carried out arrests without justification or explanation, frequently responding to detainees' requests for explanation with brutality and demanding bribes as conditions for release; SARS has also been accused of torture and other ill treatment.[20]

11. The Cybercrimes (Prohibition, Prevention, Etc) Act 2015 sets out a separate regime for communications surveillance. Where there are "reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings,"[21] a judge may order a service provider (any entity providing access to the internet) to intercept, collect, record, permit, or assist authorities in collecting or recording content or traffic data associated with specific communications,[22] or authorise a law enforcement officer to collect or record the same.[23]

Absence of Test of Necessity or Proportionality

12. International human rights standards require that every communications surveillance determination is made on the grounds that the surveillance is necessary to achieve a legitimate aim and proportionate to the aim pursued.[24] Neither the Terrorism (Prevention) Act nor the Cybercrimes (Prohibition, Prevention, Etc) Act prescribes such a test of necessity and proportionality and instead grants the authorising judge broad discretion to order surveillance measures.

13. In the Terrorism (Prevention) Act, vague terms compound this concern and allow for a wide interpretation of the types of actions that could justify issuing an order. The judge is empowered to issue an order for "intelligence gathering," though the legislation provides little guidance on what qualifies as intelligence, apart from stating that "[t]he law enforcement and security agencies . . . shall be responsible for the gathering of intelligence and investigation of the offences provided under this Act."[25] If "intelligence gathering" is read as information relating to the offences contained within the Act, those offences include, among other things, acts of terrorism;[26] assistance, facilitation, or organisation of persons or

19 See discussion below in "Monitoring of Online Activity."
20 "You Have Signed Your Death Warrant," Amnesty International, 2016, available at https://www.amnestyusa.org/files/nigeria_sars_report.pdf.
21 Cybercrimes (Prohibition, Prevention, Etc) Act 2015, s 39.
22 Ibid, s 39(a).
23 Ibid, s 39(b).
24 See "Legality," "Legitimate Aim," Necessity," "Adequacy," and "Proportionality," International Principles on the Application of Human Rights to Communications Surveillance.
25 Terrorism (Prevention) Act 2011, s 1A(3).
26 Ibid, s 2(a).

organisations engaged in terrorism;[27] and provision of training and instruction to terrorist groups or terrorists, among others.[28] The definition of "acts of terrorism" is relatively broad, and could encompass a wide range of acts, thereby creating significant room for abuse.[29]

Lack of User Notification

14. According to international human rights standards, as a general rule, every person who is subject to surveillance should be notified of the decision authorising surveillance; delays may be justified only in limited circumstances, such as when notification would seriously jeopardise the purpose of the surveillance, and for a limited time, usually until the reason for the delay no longer exists.[30] However, there is no provision in either piece of legislation requiring authorities to notify individuals or groups that they are or have been the subject of authorisation. Applications under either Act are "ex parte," meaning that the targeted person or group is not notified about the proceeding or represented at it.[31] Consequently, individuals may only become aware that they have been under surveillance if they are charged with a criminal offence and evidence obtained through surveillance is presented in court. In all other cases, there is no official route by which they may be notified of the surveillance decision, greatly undermining the possibility of obtaining redress for illegal surveillance through the courts. If an individual does not know they have been subject to surveillance measures, then effectively they have no access to a remedy if those surveillance measures violated their right to privacy.

Concerns around Transparency, Oversight, and Judicial Independence

15. International human rights standards also highlight the importance of transparency in communications surveillance determinations, in the form of published reports containing aggregated information on authorisations, and public oversight through independent oversight mechanisms that have the ability to hold authorities accountable.[32] Neither the Terrorism (Prevention) Act nor the Cybercrimes (Prohibition, Prevention, Etc) Act mandate transparency or establish independent oversight mechanisms. There do not appear to have been any public statements on the number of times that orders have been made under either Act or in relation to the number of people affected. Robust transparency measures allow for public scrutiny and the ability to assess whether powers are being appropriately used, while public oversight ensures that unlawful actions are investigated and reported on. Security agencies in

27 Terrorism (Prevention) Act 2011, s 2(f).
28 Ibid, s 7.
29 Ibid, s 29 (referencing s 1).
30 See "User Notification," International Principles on the Application of Human Rights to Communications Surveillance.
31 Terrorism (Prevention) Act 2011, s 29(1); Cybercrimes (Prohibition, Prevention, Etc) Act 2015, s 45(1).
32 See "Transparency" and "Public Oversight," International Principles on the Application of Human Rights to Communications Surveillance.

Nigeria are reportedly poorly overseen, with legislative oversight largely limited to budgetary approvals.[33]

16. Under international human rights standards determinations concerning communications surveillance must be made by a competent authority (preferably judicial) that is independent and impartial.[34] Although the decision to authorise communications surveillance under either the Terrorism (Prevention) Act or Cybercrimes (Prohibition, Prevention, Etc) Act is made by a judge, it remains to be seen whether the Nigerian judiciary is fully independent and impartial. In a 2014 report, Human Rights Watch noted that while "[t]he [Nigerian] judiciary remained nominally free from interference and pressures from other branches of government . . . corruption did impede pursuit of justice."[35] The report further characterised the judiciary as "weak and overburdened."[36] With the threat posed by Boko Haram, judicial independence may come under particular pressure in the counterterrorism context.

Concerns about Indiscriminate Data Retention

17. In Nigeria, regulatory guidance requires internet service providers to "retain internet service related information, including user identification, the content of user messages and traffic or routing data, for a minimum period of twelve (12) months or as otherwise directed by the Commission from time to time."[37] The Human Rights Committee has confirmed that data retention policies constitute an interference with the right to privacy and that as a general rule states should "refrain from imposing mandatory retention of data by third parties."[38] Further, data retention has significant implications for the right to freedom of expression, particularly as mandatory data retention de facto limits the capacity of individuals to remain anonymous.[39]

18. The Cybercrimes (Prohibition, Prevention, Etc) Act specifically requires service providers to "keep all traffic data and subscriber information . . . for a period of 2 years,"[40] and to comply with requests of law enforcement agencies or

33 See Jude Uddoh, "Corruption Risks in Nigeria's Defence and Security Establishments: An Assessment," 2016, p 2003.

34 See "Competent Judicial Authority," International Principles on the Application of Human Rights to Communications Surveillance, 2014, available at https://en.necessaryandproportionate.org/.

35 "World Report 2014: Nigeria," Human Rights Watch, 2014, available at https://www.hrw.org/world-report/2014/country-chapters/nigeria.

36 Ibid. See also Philip C. Aka, "Judicial Independence under Nigeria's Fourth Republic: Problems and Prospects," California Western International Law Journal, 2014, available at https://scholarlycommons.law.cwsl.edu/cwilj/vol45/iss1/2.

37 Nigerian Communications Commission, Guidelines for the Provision of Internet Service, https://www.ncc.gov.ng/docman-main/legal-regulatory/guidelines/62-guidelines-for-the-provision-of-internet-service/file.

38 Concluding Observations of the Fourth Periodic Report of the United States of America, Human Rights Committee, U.N. Doc. CCPR/C/USA/CO/4, para 22 (23 April 2014).

39 See report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/29/32 (22 May 2015), noting at paragraph 55: "Broad mandatory data retention policies limit an individual's ability to remain anonymous. A State's ability to require Internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint."

40 Cybercrimes (Prohibition, Prevention, Etc) Act 2015, s 38(1).

relevant authorities for the preservation and release of data.[41] Paradigm Initiative has challenged the constitutionality of this requirement.[42] Collection and analysis of metadata—such as traffic data, which can include information that identifies individuals and locations, among other things—is as intrusive as collection and analysis of the content of communications. States across the world continue to subject interception of and access to metadata to no or significantly lower safeguards than the content of communications, despite the recognition by the United Nations Human Rights Council that "metadata, when aggregated, can reveal personal information that can be no less sensitive than the actual content of communications."[43] In particular, mandatory obligations on telecommunications companies and internet service providers to retain the data of their subscribers in an untargeted and indiscriminate manner violate human rights standards.

Proposed Legislation Governing Communications Surveillance

19. The government has stated that it plans to establish a new legal regime for interception of communications, but there are concerns that proposed legislation in its current form does not provide for effective protection of privacy in practice. In 2013, the Nigerian Communications Commission ("NCC"), the regulatory authority for Nigeria's telecommunications industry, introduced a Draft Lawful Interception of Communications Regulation.[44] If brought into force, this regulation would enable interception of communications—both with and without a warrant[45]—and require mobile phone companies to retain intercepted voice and data communications for three years.[46] It would also require telecommunications licensees to provide specified security agencies with access to protected communications virtually on demand.[47]

20. Under the regulation, a warrant would be "necessary" if it was in the interests of national security[48] or for the purpose of preventing or investigating a crime,[49] among other reasons. However, a specified security official could initiate interception of communications without a warrant in some circumstances (for example, if he deemed that there had been an emergency involving immediate danger of death or serious injury to any person[50]), although he would be required to apply for a warrant within 48 hours after the interception began.

41 Cybercrimes (Prohibition, Prevention, Etc) Act 2015, s 38(2).
42 See "PIN Calls for Immediate Release of Arrested Blogger and Review of Cybercrime Law," Paradigm Initiative, 9 August 2016, available at https://pinigeria.org/pin-calls-for-immediate-release-of-arrested-blogger-and-review-of-cybercrime-law/; "Expert Condemns Abuse of Cybercrimes Law to Harass Citizens," Paradigm Initiative, 12 March 2018, available at https://pinigeria.org/expert-condemns-abuse-of-cybercrimes-law/.
43 Human Rights Council resolution on the right to privacy in the digital age, UN doc. A/HRC/RES/34/7.
44 Nigerian Communications Commission, Draft Lawful Interception of Communications Regulations, 2013, available at https://www.ncc.gov.ng/docman-main/legal-regulatory/regulations/drafts-regulations/328-lawful-interception-of-comunications-regulations/file.
45 Ibid, cls 3, 4.
46 Ibid, cl 18.
47 Ibid, cl 10.
48 Ibid, cl 5(3)(a).
49 Ibid, cl 5(3)(b).
50 Ibid, cl 7(4)(a).

21. The proposed regulation has prompted significant controversy.[51] Concerns include that it uses vague language that could be interpreted arbitrarily, and that it would give numerous unsupervised powers to the NCC, while failing to require public reports on interception decisions.[52] As of March 2018, there do not appear to be concrete plans for the adoption of this regulation, but civil society groups remain concerned that the proposal could be revived.

Surveillance Capabilities

22. Budget appropriations suggest that surveillance is a major activity of the Nigerian state. In 2017 alone, Nigeria spent nearly NGN 46 billion ($127.6 million USD) on surveillance capabilities.[53] Further, in January 2018, the Nigerian Ministry of Budget and National Planning announced a plan to allocate NGN 2.21 billion ($6 million USD) to the DSS for monitoring social media accounts.[54]

23. CitizenLab, an interdisciplinary laboratory at the University of Toronto, has found evidence to suggest the existence of FinFisher Command & Control servers[55] in Nigeria since at least May 2013.[56] FinFisher is an advanced spyware program sold exclusively to governments and supplied by British company Gamma International. The program relies on a network of disguised servers to provide direct access to a target's device, which allows the person monitoring to retrieve offline data from the device, follow encrypted communications, and identify the location of the target, while concealing the location of those actually receiving the collected information. Although FinFisher has been marketed as a legitimate crime-fighting tool, international experience suggests that it can be used in contravention of international human rights standards.[57] Nigeria is also believed to be a client of Blue Coat Systems, a company with links to the surveillance programs of many oppressive regimes.[58] Blue Coat's technology provides for deep packet inspection, which enables analysis of internet traffic for surveillance, tracking,

51 See "Report of the Public Inquiry on the Lawful Interception of Communications Regulations," Nigerian Communications Commission, 2015, available at https://www.ncc.gov.ng/docman-main/legal-regulatory/public-inquiries/660-public-inquiry-on-lawful-interception-of-communications-regulations/file.

52 See "Reality Check: Status of Internet Freedom in Nigeria," Paradigm Initiative, 2015, available at https://ng.boell.org/sites/default/files/uploads/2016/01/internet_freedom_in_nigeria.pdf.

53 "Status of Surveillance in Nigeria: Refocusing the Search Beams," Paradigm Initiative, 2017, available at http://pinigeria.org/2016/wp-content/uploads/documents/policy/%28Policy%20Brief%20009%29%20Status%20of%20Surveillance%20in%20Nigeria.pdf.

54 "DSS to monitor Facebook, Twitter- Minister," Metrostarng, 20 January 2018, available at http://metrostarng.com/news/dss-monitor-facebook-twitter-minister/.

55 For further details, see "FinFisher" in the Surveillance Industry Index, developed by Privacy International hosted by Transparency Toolkit. https://sii.transparencytoolkit.org/docs/Gamma-Group_FinFisher_Brochure_0sii_documents.

56 Morgan Marquis-Boire et al, "For Their Eyes Only: The Commercialization of Digital Spying," CitizenLab, 1 May 2013, available at https://citizenlab.ca/storage/finfisher/final/fortheireyesonly.pdf.

57 Bill Marczak et al, "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation," CitizenLab, 15 October 2015, available at https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/.

58 Morgan Marquis-Boire et al, "Planet Blue Coat: Mapping Global Censorship and Surveillance Tools," CitizenLab, 15 January 2013, available at https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/.

filtering, and censorship online. Although these technologies are marketed exclusively to governments, there is no indication of which bodies in Nigeria may have purchased or used them.

24. There have been additional reports of troubling surveillance activities conducted in Nigeria. In 2017, news reports pointed to the existence of a government program conducting surveillance of mobile phones in Nigeria's capital, Abuja.[59] In addition, reports have noted the Nigerian government's planned launch of communications satellites with possible "eavesdropping" capabilities.[60] While the true capabilities of the satellites remain unknown, Paradigm Initiative has attempted to obtain such information through filing a Freedom of Information request with the Federal Ministry of Science and Technology.[61] After the Ministry failed to comply with Paradigm Initiative's request, Paradigm Initiative took the matter to court and the matter remains pending as of March 2018.[62]

Monitoring of Online Activity

25. Recent developments indicate increased monitoring of online activities—particularly social media—by government actors. On 23 August 2017, the Director of Defence Information announced the military's plan to monitor social media activities[63] from strategic media centers "to sieve out and react to [speeches] that will be anti-government, be anti-military, and be anti-security."[64] This announcement occurred two days after President Muhammadu Buhari condemned some online speech as "cross[ing]… red lines."[65] On 25 January 2018, the Minister of Defense issued a directive ordering security agencies to "tackle the propagation of hate speeches through the social media."[66]

26. These developments contribute to an atmosphere of fear of surveillance, especially in light of speech-related arrests recently carried out by security

59 "DSS Bugs 70% of Mobile Phones In Abuja," Independent NG, 8 November 2017, available at https://independent.ng/dss-bugs-70-mobile-phones-abuja/.

60 "CSO Raises Alarm, Sues FG for Spying on Nigerians with Satellites," Nigeria Communications Week, 20 June 2017, available at http://nigeriacommunicationsweek.com.ng/cso-raises-alarm-sues-fg-for-spying-on-nigerians-with-satellites/.

61 See "Press Release: Paradigm Initiative Makes FOI Request on Nigeria's 'Eavesdropping Satellites," Paradigm Initiative, 2 February 2017, available at https://pinigeria.org/foi-eavesdrop-satellite-ng/.

62 "CSO Raises Alarm, Sues FG for Spying on Nigerians with Satellites," Nigeria Communications Week, 20 June 2017, available at http://nigeriacommunicationsweek.com.ng/cso-raises-alarm-sues-fg-for-spying-on-nigerians-with-satellites/.

63 For more information on social media monitoring, refer to Privacy International's explainer available at https://privacyinternational.org/explainer/55/social-media-intelligence.

64 "Military now monitoring comments on social media – Defence Spokesman," The Defender, 23 August 2017, available at http://www.thedefenderngr.com/military-now-monitoring-comments-on-social-media-defence-spokesman/.

65 Isiaka Wakili, "Transcript Of President Buhari's Speech: Nigeria's Unity Settled," Sahara Reporters, 21 August 2017, available at http://saharareporters.com/2017/08/21/transcript-president-buharis-speech-nigeria's-unity-settled.

66 Gbenga Bada, "Security agencies to monitor and tackle spread on social media," Pulse, 25 January 2018, available at http://www.pulse.ng/news/local/security-agencies-to-monitor-hate-speeches-on-social-media-id7893643.html.

agencies. For example, in April 2017, DSS arrested a man named Chisom Anaele at his home, allegedly because of comments he had made on social media.[67] On 1 January 2018, SARS agents arrested Nigerian publishers Daniel Elombah and Tim Elombah.[68] The cause of the arrest, as allegedly disclosed by SARS agents, was an online article criticising the Inspector General of Police, which the government attributed to Tim Elombah.[69]

27. Nigerian civil society groups have expressed strong concerns regarding this trend. For example, the Partnership for Media and Democracy has criticised the military's decision to monitor social media as creating "enormous opportunities for abuse of power and the violation of the fundamental rights and freedoms of Nigerians."[70] The government has defined the communications that warrant monitoring in vague terms, giving little guidance as to the meaning of phrases such as "hate speech" and "red lines." Further, the power to monitor online activities is dispersed among multiple authorities, such as DSS and the military, with no suggestion that their conduct will be adequately checked by oversight, triggering concerns that monitoring will not comply with international best practices.

28. Governments and companies argue that monitoring social media and other information individuals post online has little impact on privacy as and when they rely "only" on publicly available information. This inaccurate representation fails to account for the intrusive nature of collection, retention, use, and sharing of personal data obtained through social media. By way of example, "tweets" posted from a mobile phone can disclose location data, and their content can also reveal individual opinions (including political opinions), as well as information about a person's preferences, sexuality, and health status.[71]

II. Data Protection Concerns

29. Nigeria does not have overarching data protection legislation; nor has any agency been charged with administering the country's overall data protection regime. Best practices suggest that an effective data protection regime depends on comprehensive data protection legislation and the existence of a well-resourced and independent authority to ensure consistent application of rules and maintain the accountability of organisations that engage in the processing of personal data. Major information collecting agencies include the National Identity Management Commission, the NCC, and the Central Bank of Nigeria. The protections these agencies offer for personal information

67 Thandiubani, "How DSS Arrested Man Over Social Media Comment and Kept Him in Custody for Over 3 Months," Tori, 9 August 2017, available at https://www.tori.ng/news/70214/how-dss-arrested-man-over-social-media-comment-and.html.

68 Daniel Elombah, "I Was Abducted By SARS – Daniel Elombah," ElombahNews, 4 January 2018, available at https://elombah.com/index.php/special-reports/i-was-abducted-by-sars-daniel-elombah/.

69 Ibid.

70 "Media Rights Group Condemns Nigerian Government's Threat To Monitor Social Media," Sahara Reporters, 31 August 2017, available at http://saharareporters.com/2017/08/31/media-rights-group-condemns-nigerian-government's-threat-monitor-social-media.

71 See "Explainer: Social Media Monitoring," Privacy International, available at: https://privacyinternational.org/explainer/55/social-media-intelligence

(such as individuals' names, medical information, and biometric data) vary in accordance with the specific laws or regulations that govern each agency's data processing and often fall short of international best practices on data protection.

Inadequate Protection of Personal Information by Data Collecting Agencies

National Identity Card Scheme

30. The National Identity Management Commission ("NIMC") plays a foundational role in Nigeria's identity regime. Under the law establishing the agency ("NIMC Act"), the NIMC is charged with establishing a National Identity Database[72] and issuing identity cards.[73] All Nigerian citizens (and some non-nationals living in Nigeria[74]) are required to participate[75] and provide biometric information (ten fingerprints and facial images).[76] Failure to register is punishable by fines and / or imprisonment.[77] As of January 2018, the NIMC has already enrolled over 28 million people, and aims to extend the scope of enrolment to 78 million by December 2018 (Nigeria's total population is 186 million people).[78]

31. By way of protection, the NIMC Act prohibits third-party access to the information stored in the database except with the consent of both the NIMC and the person whose information is sought.[79] Unlawful access is punishable by imprisonment of ten years without the option of fine.[80] Despite this general prohibition, the NIMC is permitted to provide "another person" (a term that is not defined in the legislation) with personal information when disclosure is in the interests of national security, when disclosure is necessary for purposes related to crime prevention or detection, or when disclosure is for purposes "strictly necessary in the public interest" as specified under an NIMC regulation.[81] Several concerning features exist in the legislation. First, although it prohibits unauthorised access, the NIMC Act does not spell out the NIMC's own duty to implement security safeguards.[82] Second, the Act contains no mechanism for holding the NIMC accountable for its protection of individuals' personal information—for example, if the NIMC unlawfully releases an individual's information, there is no mechanism for that individual to complain or seek a remedy.[83]

32. Additionally, the Act is silent on the regulation of subcontractors and the

[72] National Identity Management Commission Act 2007, s 14(1).
[73] Ibid, s 18(5).
[74] Permanent residents and non-national residents who are resident for two or more years.
[75] National Identity Management Commission Act 2007, s 18(1).
[76] Ibid, s 14(2).
[77] Ibid, s 30(1)(a).
[78] "NIMC Enrolls Over 28m Nigerians and Legal Residents," National Identity Management Commission, 29 January 2018, available at https://www.nimc.gov.ng/nimc-enrols-over-28m-nigerians-and-legal-residents/.
[79] National Identity Management Commission Act 2007, s 26(1).
[80] Ibid, s 28(2).
[81] Ibid, s 26(2)-(4).
[82] See Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD, 11 July 2013, para 11, available at http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.
[83] See ibid, para 14.

restriction of cross-border data transfers. The absence of a robust data protection mechanism can subject citizens to profound risks, especially when foreign contractors are engaged, as illustrated by the national identity card scheme's turbulent history.[84] Various unsuccessful attempts have been made to roll-out a national identify card scheme in Nigeria since one was first proposed in 1976. The most recent attempt prior to the current effort took place between 2001 and 2006; it ended in a corruption scandal in which the technology subcontractor, SAGEM (a French company), was terminated for breach of contract and bribery of Nigerian officials.[85] At the point of termination, SAGEM had collected the personal information of 35 million Nigerians.[86] SAGEM's status as a foreign company prevented the Nigerian government from exerting meaningful control over its conduct after project termination.

33. The current national identity card project is a fresh attempt that involves redoing all the data collection completed by SAGEM.[87] Like its predecessors, the NIMC enlists the assistance of subcontractors, including foreign companies, most notably MasterCard.[88] While it has been reported that MasterCard will limit its involvement in the identity card scheme to supporting the card's payment function and will not store biometric data,[89] given the lack of comprehensive data protection legislation, concerns remain regarding the protection of Nigerians' personal information.[90]

34. The national identity card may also play a role in elections. Nigeria is amending its Electoral Act 2010 to allow electronic voting in the 2019 general election[91] and the NIMC has indicated that the card could be used in that election.[92] If this transpires, the safety of Nigerians' personal data should be prioritised, particularly in light of the fact that a mass disclosure of voter information did occur in 2016, when voter data collected by the Independent National Electoral Commission was published on a third-party website.[93]

84 Nicholas Ibekwe, "Over N121 billion wasted, Nigeria's troubled National ID Card project in fresh controversy," Premium Times, 27 May 2015, available at https://www.premiumtimesng.com/news/headlines/183720-over-n121-billion-wasted-nigerias-troubled-national-id-card-project-in-fresh-controversy.html.

85 Ibid. See also "Identification for development (ID4D): identification systems analysis – country assessment Nigeria," World Bank Group, June 2015, p 1, available at http://documents.worldbank.org/curated/en/136541489666581589/pdf/113567-WP-P156810-PUBLIC-1618628-Nigeria-ID4D-Web.pdf.

86 Nicholas Ibekwe, "Over N121 billion wasted, Nigeria's troubled National ID Card project in fresh controversy," Premium Times, 27 May 2015, available at https://www.premiumtimesng.com/news/headlines/183720-over-n121-billion-wasted-nigerias-troubled-national-id-card-project-in-fresh-controversy.html.

87 "NG: New National Identity Card!", The Nation, 18 July 2011, available at http://ifg.cc/aktuelles/nachrichten/regionen/173-ng-nigeria/35356-ng-new-national-identity-card.

88 "MasterCard-Branded National eID Card Launched in Nigeria," MasterCard, 28 August 2014, available at https://newsroom.mastercard.com/press-releases/mastercard-branded-national-eid-card-launched-nigeria/.

89 Jesse Oguntimehin, "Implications of Nigeria's National ID Card," iAfrikan, 30 September 2014, available at https://www.iafrikan.com/2014/09/30/nigeria-national-id-card/.

90 Lukman Adebisi Abdulrauf et al, "New Technologies and the Right to Privacy in Nigeria: Evaluating the Tension between Traditional and Modern Conceptions," 7 Nnamdi Azikiwe U. J. Int'l L. & Juris, 2016, p. 119, available at https://www.ajol.info/index.php/naujilj/article/download/136246/125736.

91 "Major highlights of Electoral Act amended by Senate," Daily Trust, 1 April 2017, available at https://www.dailytrust.com.ng/news/for-the-record/major-highlights-of-electoral-act-amended-by-senate/191685.html.

92 "We are ready for e-voting – NIMC," The Nation, 28 November 2016, available at http://thenationonlineng.net/ready-e-voting-nimc/.

93 Olusegun Ogundeji, "Nigeria: Electoral Commission accused of data security blunder," ITWeb Africa, 27 September 2016, available at http://www.itwebafrica.com/security/511-nigeria/236853-nigeria-electoral-commission-accused-of-data-security-blunder.

Databases Maintained by Other Authorities

35. An array of other authorities, such as the NCC, the Central Bank of Nigeria ("Central Bank"), the Independent National Electoral Commission, the Federal Road Safety Corps, and the Nigerian Immigration Service, have established their own identity registration programs in parallel to NIMC's national identity database. Aspects of these databases and their management raise concerns regarding potential abuses and unauthorised disclosures. One example is the Central Bank's Bank Verification Number ("BVN") project, which potentially puts millions of Nigerians' biometric data at risk.

36. The BVN project attempts to create a unique identity number for each Nigerian that can be used across the finance industry.[94] This is to be achieved by requiring financial institutions to capture customers' biometric and demographic information and transmit the information[95] to a central database.[96] Data collection is mandatory, as evidenced by stringent measures taken by the federal government to compel the compliance of financial institutions.[97] As of February 2017, nearly 52 million individuals have been registered in the BVN system.[98]

37. Despite entailing a massive aggregation of biometric information, the BVN project contains few mandatory data security measures[99] and falls short of adequately protecting banking customers' personal information. First, the Central Bank directive governing the project relies on broad terms (such as "adequate" and "secure") to define data collecting entities' security obligations. Financial institutions have little guidance as to what safeguards are called for when they collect sensitive information from customers. Second, the directive fails to specify any monitoring mechanisms (such as reporting and inspection) to ensure financial institutions' data protection compliance. Third, in contrast to laws passed by the national legislature, the BVN directive is issued by the Central Bank itself,[100] which diminishes the document's potential to be an adequate basis for holding the Central Bank accountable with respect to data protection.

94 Regulatory Framework for Bank Verification Number (BVN) Operations and Watch-list for the Nigerian Banking Industry, para 1.1; see also Rotimi Akapo, "Proliferation of Data Collection and Storage Agencies in Nigeria – Data Protection and privacy issues," Advocaat Law Practice, November 2017, available at http://www.advocaat-law.com/assets/resources/acf4ebf030a90b61d7d16979921b9360.pdf.

95 Regulatory Framework for Bank Verification Number (BVN) Operations and Watch-list for the Nigerian Banking Industry, paras 1.4.1.3(i), 1.5(i).

96 Ibid, para 1.4.1.2(iv).

97 Onome Ohwovoriole, "FG obtains court order seizing funds in accounts with no BVN/Incomplete KYC," 21 October 2017, available at https://nairametrics.com/federal-government-obtains-court-order-to-seize-money-in-account-with-no-bvnincomplete-kyc/.

98 Obinna Chima, "51.72m Bank Customers Enrolled on BVN as at February," This Day, 22 March 2017, available at https://www.thisdaylive.com/index.php/2017/03/22/51-72m-bank-customers-enrolled-on-bvn-as-at-february/.

99 These measures include requirements for (i) secured hardware and software and message encryption, (ii) local storage of data storage and limited cross-border routing, (iii) "adequate security procedures" and (iv) classification of information as confidential. See Regulatory Framework for Bank Verification Number (BVN) Operations and Watch-list for the Nigerian Banking Industry, para 1.8(i)-(iv).

100 Rotimi Akapo, "Proliferation of Data Collection and Storage Agencies in Nigeria – Data Protection and privacy issues," Nairametrics, November 2017, available at http://www.advocaat-law.com/assets/resources/acf4ebf030a90b61d7d16979921b9360.pdf.

Harmonisation Scheme

38. Nigeria's fragmented data processing regime has long been criticised for wasting taxpayer funds and unnecessarily burdening Nigerians. In October 2013, then President Goodluck Jonathan issued a directive calling for the harmonisation of the nation's identity databases and requesting that "all government agencies requiring identity verification and authentication services or involved in data capture activities must align their activities with a view to switching over to the NIMC infrastructure."[101] This order was renewed by President Buhari through a 2015 directive, which again called for establishing a centralised database administered by NIMC.[102] In September 2017, the government announced that government actors planned to fully harmonise all existing identity databases within 14 months, starting with the BVN database, the NCC database (discussed below), and the database maintained by the Federal Road Safety Commission.[103] As of March 2018, the scheme appears to be proceeding but its status is unclear.

39. Data harmonisation serves the laudable objective of reducing fiscal waste and eliminating duplicate registrations, but can also trigger data protection concerns that compound in the absence of legal and institutional measures to ensure data protection principles are respected. When previously independent databases are merged into the NIMC database, the amount of personal information at stake and the number of people who can access it increases. This can significantly drive up risks of abuse, and the potential for data to be used in ways that were never intended when it was collected.[104] As they stand now, the NIMC Act and NIMC's internal privacy policy fail to integrate necessary safeguards to protect the integrity and security of the data and the infrastructure. It is therefore imperative that the government enhance data protection measures around the NIMC database as an integral part of the harmonisation program.

SIM Registration Scheme

40. Under the NCC's Registration of Telephone Subscribers Regulation 2011 ("RTS Regulation"), mobile telephone service providers are required to capture and register biometric information (facial images and fingerprints) and other personal information of telephone subscribers, and transmit such information to a central

101 Niyi, "Register All Nigerians by Dec, 2014, Jonathan Orders NIMC," Information Nigeria, 18 October 2013, available at http://www.informationng.com/2013/10/register-all-nigerians-by-dec-2014-jonathan-orders-nimc.html.

102 "Data Collection Agencies Get Presidential Order to Aggregate Databases," National Identify Management Commission, available at https://www.nimc.gov.ng/data-collection-agencies-get-presidential-order-to-aggregate-databases/.

103 Aanuoluwa Omotosho et al, "Nigerian Government Moves To Harmonise Data From NCC, FRSC, CBN," IT Edge News, 24 September 2017, available at https://itedgenews.ng/2017/09/24/nigerian-government-moves-harmonise-data-ncc-frsccbn/.

104 "Identification for development (ID4D): Identification system analysis – country Assessment Nigeria," World Bank Group, June 2015, p 51, available at http://documents.worldbank.org/curated/en/136541489666581589/pdf/113567-WP-P156810-PUBLIC-1618628-Nigeria-ID4D-Web.pdf.

database maintained by the NCC.[105] Mobile telephone service providers are further required to deactivate existing subscriptions upon the NCC's request if the subscribers' information is not entered into the central database within a designated grace period.[106] In October 2016, the NCC imposed a NGN 1.04 trillion fine ($5.2 billion USD) on a major operator named MTN for its failure to disconnect 5.1 million unregistered SIMs.[107]

41. Compulsory SIM card registration and the retention of information about mobile phone users in a centralised database threaten the right to privacy. SIM card registration undermines the ability of users to communicate anonymously and disproportionately disadvantages the most marginalised groups in a society.[108] It can have a discriminatory effect by excluding users from accessing mobile networks. It also facilitates surveillance and makes tracking and monitoring of users easier for authorities, concerns that are especially acute in countries with conflict, political instability, and civil society suppression.

42. The RTS Regulation has also triggered concerns regarding cross-border transfer with inadequate safeguards of personal data processed in Nigeria. Based on the RTS Regulation, mobile service providers can retain non-biometric subscriber information after transmitting that information to the central database.[109] Notably, the largest mobile service provider in Nigeria, MTN, is a South African company.[110] By virtue of its compliance with the RTS Regulation, MTN has obtained the personal information of more than 40 million Nigerian subscribers.[111] Concern has arisen that such data is readily accessible by MTN's head office in South Africa.[112] Although the RTS Regulation prohibits cross-border transfers of subscriber information without NCC's authorisation,[113] it has not spelled out the applicable penalties for violations.

Proposed Data Protection Legislation

43. Although attempts to pass laws that address privacy concerns have long been making slow progress,[114] recent events suggest that legislators may be renewing their efforts to create overarching legislation on data protection and privacy. Two privacy-related bills, the Data Protection Bill 2015 and the Digital Rights and

105 Registration of Telephone Subscribers Regulation (RTS) 2011, r 11.
106 Ibid, r 13(3).
107 Bassey Udo, "NCC-MTN fine saga: Setting a dangerous precedence?", Premium Times, 8 March 2016, available at https://www.premiumtimesng.com/business/199747-analysis-ncc-mtn-fine-saga-setting-dangerous-precedence.html.
108 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 2013, para 70; see also Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, May 2015, A/HRC/29/32, para 51.
109 Registration of Telephone Subscribers Regulation (RTS) 2011, rr 7, 9(6).
110 Asuquo Kofi Essien Allotey, "Data Protection and Transborder Data Flows: Implications for Nigeria's Integration into the Global Network Economy," UNISA Institutional Repository, February 2014, p 126, available at https://www.peacepalacelibrary.nl/ebooks/files/382580575.pdf.
111 Ibid.
112 Ibid.
113 Registration of Telephone Subscribers Regulation (RTS) 2011, r 10(4).
114 Gbenga Sesan, "Right to privacy? Nigeria needs a Data Protection Law," World Wide Web Foundation, 11 October 2017, available at https://webfoundation.org/2017/10/right-to-privacy-nigeria-needs-a-data-protection-law/.

Freedom Bill 2016, have been passed by the Nigerian House of Representatives and (as of March 2018) are undergoing review in the Senate. It is anticipated that one or both of the bills will become law in 2018.

44. The Data Protection Bill would regulate the collection, processing, storage and transfer of personal data by "data controllers," whose definition appears to cover both government and private actors. It specifies a set of data protection principles similar to those contained in the NITDA Draft Guidelines on Data Protection.[115] It also sets forth several safeguards, such as the right of individuals to be informed regarding the processing of their data, but leaves important aspects untouched. For example, the bill does not specify the mechanisms for ensuring accountability.[116] The Digital Rights and Freedom Bill would similarly establish a new data protection regime. Among other measures, it would create a new mechanism for victims of violations to bring court cases and designate an agency to oversee data protection matters.[117]

RECOMMENDATIONS

To better protect the right to privacy, we recommend that the government of Nigeria:

45. Reform the current legal framework and policies governing communications surveillance, as well as review pending legislation such as the Draft Lawful Interception of Communications Regulation, to ensure that they meet international human rights standards and in particular comply with test of legality, necessity, and proportionality.

    - Adopt and enforce a comprehensive data protection law that affirms the right to privacy; sets out procedures for lawful, fair, and secure processing of personal data; enshrines data protection rights; and provides for an independent data protection authority that is appropriately resourced and has the authority to oversee and ensure the implementation of the law.
    - Take necessary measures to strengthen independent judicial authorisation and oversight mechanisms of communications surveillance.
    - Reform Nigeria's security agencies so that they are regulated by laws that clearly prescribe their powers, establish oversight mechanisms, and meet with international human rights standards.
    - Abolish mandatory SIM card registration and review the data retention requirements placed on internet service providers.
    - Disclose what type of surveillance technologies are employed by Nigerian law enforcement and security agencies, how their acquisition and use is regulated and monitored, and how agencies are complying with Nigeria's national and international obligations.

115 See Draft Data Protection Bill, 2015, available at http://placbillstrack.org/upload/HB02.pdf.
116 Ibid.
117 See Draft Digital Rights and Freedom Bill, 2016, available at http://placbillstrack.org/upload/HB490.pdf.

- Conduct prompt and independent investigations into credible reports of unlawful surveillance of lawyers, journalists, human rights activists, and others, with the view to bringing to justice the perpetrators and providing reparations, and make publicly available the results of these investigations.
- Implement media and information literacy programs to enhance public awareness regarding the importance of privacy.