PRIVACY INTERNATIONAL

Universal Periodic Review
Stakeholder Report: 21st Session, Guinea

The Right to Privacy in Guinea

Submitted by: Privacy International, Jonction, and Stat View International

‘No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence.’

The Universal Declaration of Human Rights

PRIVACY INTERNATIONAL



SVI STAT VIEW International

Introduction

1. This stakeholder report is a submission by Privacy International (PI), Jonction and Stat View International. **Privacy International** is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world. **Jonction** is a human rights organisation based in Dakar, Senegal, which aims to promote sustainable and equitable development as well as human rights across Africa but particularly in Senegal. **Stat View International** is a research-based organisation that promotes good governance and human rights in Sub Saharan Africa. It is currently the leading organization of the Francophone Civil Society Coalition against Corruption.

2. Together PI, Jonction and Stat View International wish to bring concerns about the protection and promotion of the right to privacy in Guinea before the Human Rights Council for consideration in Guinea's upcoming review.

The right to privacy

3. Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[1] 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, ad "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals.[2] Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, are necessary to achieve a legitimate aim, and are proportionate to the aim pursued.[3]

4. 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 a number of State obligations related to the protection of personal

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

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

[3] Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

data.[4] A number of international instruments enshrine data protection principles,[5] and many domestic legislatures have incorporated such principles into national law. Data protection is also emerging as a distinct human or fundamental right: numerous countries in Latin America and Europe have now recognised data protection as a constitutional right, and the recently adopted ASEAN Human Rights Declaration explicitly applies the right to privacy to personal data (Article 21). At the sub-regional level, in 2010 the Economic Community of West African States (ECOWAS) has adopted a Supplementary Act on the protection of personal data[6], which has been adopted and implemented by several countries, such as Benin, Ghana but it is yet to be adopted by Guinea.

Follow up to the previous UPR

5. There was no mention of the right to privacy and data protection, and the resulting violations in the National Report submitted by Guinea or in the final report of the Working Group on the occasion of Guinea's review in 2010.

International obligations related to privacy

6. **Article 151** of the **Constitution of Guinea**[7] states that international law takes precedence over domestic law. Guinea is a signatory to the Universal Declaration of Human Rights ('UDHR') and party to the International Covenant on Civil and Political Rights ('ICCPR'). Article 17 ICCPR provides for the right to freedom from arbitrary interference with privacy, family, home and correspondence.

Domestic laws and regulations related to privacy

7. **Article 12** of the **Constitution of Guinea** protects the privacy of the home and of communications, stating:

> *"The domicile is inviolable.*
>
> *It may be infringed only in the case of grave and imminent peril, to evade a common danger or to protect the life of the persons. All other infringement,*

[4] Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17).
[5] See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co- operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72)
[6] Supplementary Act A/SA.1/01/10 on Personal Data Protection Within ECOWSAS. Available at: http://www.ecowas.int/publications/en/actes_add_telecoms/SIGNED-Personal_Data.pdf
[7] Constitution of the Republic of Guinea of 2010, available at: https://www.constituteproject.org/constitution/Guinea_2010.pdf

all search may only be ordered by the judge or by the authority that the law designates and in the forms prescribed by it.

The secrecy of correspondence and of communication is inviolable. Each one has the right to the protection of their private life."

8. **The Telecommunications Act of Guinea**[8] includes several provisions that protect the right to privacy and personal data. For example, **Article 42** notes the obligation of service providers to respect laws protecting individual freedoms and private life.

Areas of Concern

1. Absence of data protection law

9. Guinea does not have a law regulating the protection of personal data, and there is no independent data protection authority. Each state institution separately regulates privacy within their remit of work. For example, the Ministry of Security is responsible for the Civil Registry; the National Communication Council for all the information that is published by the press; and the Ministry of Communication for data collected for SIM card registration. Biometric technology is utilised by a variety of government agencies: in data collection and management systems used by the Ministry of Security for biometric passports, for the enrolment of voters by the National Independent Electoral Commission, and in the management of the national labour force by the Ministry of Public Function.

10. Government authorities have extensive access to personal data, but lack the necessary frameworks to govern that access. For example, private and public entities are not required to register activities which entail the collection, storage, and sharing of personal data. In addition, the lack of a data protection authority means there are limited or no opportunities for individuals to receive information on their right to privacy and the protection of their personal data, nor to seek redress, or compensation in case of a violation of these rights. By failing to protect personal data, Guinea is not *"ensur[ing] that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant"*.[9]

11. In light of the increasing amassment of personal data and the use of biometric technology, we urge the government to address the issue of data protection and privacy and put relevant safeguards into legislation.

---

[8] Law of L/2005/018/AN of the 8 September 2005, adopting and promulgating the law relating to the amendment of the law L/92/016/CTRN of 2 June 1997 on the general regulation of telecommunications. Available at: http://www.arpt.gov.gn/pdf/L018.pdf

[9] Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Article 17), 4 August 1988. Available at: http://www.unhchr.ch/tbs/doc.nsf/(Symbol)/23378a8724595410c12563ed004aeecd?Opendocument

2. Registration of mobile telephony users

12. The process had already started in 2008 but in 2010, Guinea's Regulatory Authority for Posts and Telecommunications (ARPT, l'Autorité de Régulation des Postes et Télécommunications) officially requested that mobile service providers register all of their subscribers. Subscribers were requested to provide their national identity cards to process their registration.[10]SIM registration is itself problematic as it undermines the ability of users to communicate anonymously and disproportionately disadvantages the most marginalized groups. It can have a discriminatory effect by excluding users from accessing mobile networks. In Guinea, not all Guineans have a national identity card. In some cases, this is because a person has not registered to receive a card; however, there have also been shortages of identity cards[11], which means many Guineans may be excluded from registering and having a mobile device.

13. SIM card registration also facilities surveillance and makes tracking and monitoring of users easier for law enforcement authorities. Indeed, there is concern that the SIM card registration process may hide an agenda to facilitate illegal communications monitoring.[12]

3. Use of biometric technology

14. Guinea has utilised biometric technology in several sectors:
    - In 2013, Zetes, a pan-European technology company, was chosen by the Guinean government to conduct the de-duplication of biometric data from its voter registry in view of the elections that took place in September 2013.
    - As part of the government's priority to reform the army, and through Security Sector Reform (SSR) programmes[13] with the support of the United Nations Development Programme[14], in 2013 the government completed the biometric registration of the military, which it had started in December 2011. The registration of the military was designed and implemented by a South African firm, CONTIPRINT.
    - In April 2014, following the success of the military registration programme, the Guinean government announced the beginning of the biometric registration process of all public officials, starting with the police and custom officials. The

[10] Guinée Presse Info, *La vie privée des guinéens n'est pas respectée*, 22 January 2012. Available at: http://www.guineepresse.info/index.php?aid=9615
[11] Vision Guinée Info, *Pénurie de cartes d'identité: la police et Sabary technology se rejettent la responsabilité*, 22 November 2013. Available at: http://www.visionguinee.info/2013/11/22/penurie-de-cartes-didentite-la-police-et-sabary-technology-se-rejettent-la-responsabilite/
[12] Guinée Presse Info, *La vie privée des guinéens n'est pas respectée*, 22 January 2012. Available at: http://www.guineepresse.info/index.php?aid=9615
[13] This project was based on the plan of action proposed by ECOWAS, the African Union and the United Nations.
[14] PBF/GIN/B-4 Projet d'appui au processus de recensement biométrique des Forces de Défense et de Sécurité with the aim of facilitating pension management, amongst others. Available at: http://mptf.undp.org/factsheet/project/00080575

data collected includes a photo, fingerprints, and electronic signatures. Recent reporting suggests that the registration of public officials was contracted out to INOVATECH ID, a French company that specialises in the production of electronic boards.

15. The use of biometric technology can be problematic: [15]
    - The data processed is at risk of being misused and is subject to fraud;
    - It can result in misidentification and inaccuracies;
    - Its nature renders it exclusionary: the universality of the technology is yet to be proven with examples of fingerprint processing technologies failing to collect usable templates from manual labourers and facial recognition systems encountering difficulties when scanning individuals with darker skin;
    - Its unregulated retention raises questions of "function creep" (uses of biometric data for purposes for which it was not originally collected) and concerns around the safety of the data: the mere existence of stored biometric data could lead to the development of new justifications for its use and poor protection of database systems enable malicious and unlawful access.

16. In addition, whilst recognising that biometric technology may not necessarily cause harm, the policy and legal void in which it is used in Guinea fails to regulate and limit its purpose. Thus, it can potentially be used as a tool for surveillance through profiling, data mining and big data analysis.

17. An additional concern is the involvement of a non-Guinean company or foreign-based company in the collection, storage and management of personal and sensitive data. This aspect raises concerns as to the ownership of data, and the responsibility and accountability of the government and the company to protect the data from abuse, theft, and loss. Given that Guinea does not have a data protection law, it is essential that the government takes the steps necessary to ensure the protection of its citizens' personal data when engaging with third parties.

18. Additionally, the physical or digital structure in which biometric data is stored must be developed to ensure the safety of the data. If they are to be used, centralised mass data systems must be regulated by clear legislation in order to eliminate the possibility of the government or third parties (i.e. private sector actors) taking advantage of the existence of the data for (new) unforeseen purposes.

4. Unlawful searches and seizures

19. The constitution and other laws provide for the inviolability of the home and require that searches are undertaken only with duly authorised warrants. However, there are reports that the police have failed to follow legal procedures when pursuing and arresting criminal suspects. This was the experience of individuals detained during

[15] Privacy International (2013) *Biometrics: Friend or foe of privacy?* Available at: https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/biometrics_friend_or_foe.pdf

the protests in May-August 2012 and February-June 2013[16]. If such reports are true, these actions constitute a violation of international standards regarding privacy and procedure for searches and seizures.[17]

Recommendations

We recommend that the government of Guinea:

20. Adopt a law on the protection of personal data adhering to international standards. The law should, for example, include safeguards pertaining to every step of the process, from collection, to access, to retention. Specifically, it should address biometric data and the establishment of independent oversight and monitoring mechanisms to ensure the accountability and responsibility of those collecting, storing and retaining biometric data;

21. Adhere to and integrate within its national laws the Supplementary Act A SA.1 01 10 of ECOWAS on personal data;

22. Ensure that the privacy and data protection rights of mobile telephony subscribers in relation to their personal data are guaranteed;

23. Put in place measures to ensure that policies and practices of law enforcement agencies to undertake searches or seizure of property are in accordance with Article 12 of the Constitution and international human rights standards.

24. Conduct an analysis of its communications surveillance practices, polices and laws against the International Principles on the Application of Human Rights to Communications Surveillance.

[16] See US Department of State, *2012 Human Rights Report: Kenya*. Available at: http://www.state.gov/j/drl/rls/hrrpt/2012humanrightsreport/index.htm?year=2012&dlid=204127#wrapper and US Department of State, *2013 Human Rights Report: Kenya*. Available at: http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm?year=2013&dlid=220120#wrapper

[17] Code of Criminal Procedure of the Republic of Guinea, Law N° 037/An/98 of 31 December 1998. Available at: http://www.hcch.net/upload/cp_gn.pdf