PRIVACY INTERNATIONAL

Submission to Committee on Defence and Interior, Parliament of Ghana on the Interception of Postal Packets and Telecommunication Messages Bill

Ghana

Privacy International & ARTICLE 19

March 2016

Submission to Committee on Defence and Interior, Parliament of Ghana on the Interception of Postal Packets and Telecommunication Messages Bill (2015)

Privacy International & ARTICLE 19, 10 March 2016

Privacy International is a nonprofit, nongovernmental organization based in London dedicated to defending the right to privacy around the world. Established in 1990, Privacy International undertakes research and investigations into state and corporate surveillance with a focus on the technologies that enable these practices. It has litigated or intervened in cases implicating the right to privacy in the courts of the US, the United Kingdom ("U.K.") and Europe, including the European Court of Human Rights. To ensure universal respect for the right to privacy, Privacy International advocates for strong national, regional and international laws that protect privacy. It also strengthens the capacity of partner organizations in developing countries to do the same.

ARTICLE 19: Global Campaign for Free Expression (ARTICLE 19) is an independent international human rights organisation that works around the world to protect and promote the right to freedom of expression and the right to freedom of information. ARTICLE 19 monitors threats to freedom of expression in different regions of the world, as well as national and global trends and develops long-term strategies to address them and advocates for the implementation of the highest standards of freedom of expression, nationally and globally.

A summary of relevant provisions and concerns

The following observations are based only on the reading of the draft Bill on interception of postal packets and telecommunication messages (2015).

Time for Review

Avowing surveillance practices and providing a comprehensive and accessible legal framework governing communications surveillance and interception is essential in a

modern democracy. States across the world are updating laws as ICT infrastructure play a more central part in people's lives, underpins democracy, and drives economic development. It is essential that privacy and freedom of expression are prioritized within these laws; they must be accessible and publicly debated, function under the principles of necessity and proportionality, have sufficient safeguards, and be in line with international law and human rights standards.

Privacy International and ARTICLE 19 are strongly concerned therefore that only three weeks has been provided for the public to debate the Bill. We are also concerned about the apparent lack of accessibility to the Bill. We strongly recommend therefore that the Bill be updated, and another public consultation be initiated with sufficient time allowed for review.

Purposes for interception

The draft Bill allows interception for the purposes of “protecting national security” (Article 2(a)) and for “fighting crime generally” (Article 2(b)). However, these terms are not defined anywhere in the Bill. Both can be used to cover a wide range of activities, leaving individuals without meaningful guidance as to which conducts might trigger surveillance.

This lack of definitions is of significant concerns as it may lead to abuses.

In particular, the draft Bill does not refer to any other Ghanaian laws that may define “national security”. The lack of definition leaves the authorities almost unlimited discretion in determining what conduct may trigger the need to interception to protect national security, what is the threshold of such threat and whether or not the threat is serious enough to justify secret surveillance.

Unclear role of the judge in authorising an interception warrant

The procedure for interception envisaged in the draft Bill includes reference to seeking an interception warrant by a Justice of the High Court (Article 4.1). However, nowhere in the draft Bill is specified the role of the judge in authorising such warrants.

There is no indication as to what test the judge should apply in deciding whether or not to authorise the interception and what safeguards he/she can impose, or any role in supervising the execution of the interception warrant. Further, Article 5 requires that sufficient information is provided to the National Security Co-ordinator in order to determine whether the conditions to grant authorisation have been satisfied. However, there is no provision requiring the judge to review such information. And Article 6 requires

an officer nominated by the National Security Co-ordinator to consider the application and make the necessary inquiries before submitting their opinion on whether the request fulfil the relevant conditions.

Prima facie then, it seems that there is no role given to a judge in reviewing and assessing the information in support for an interception warrant. The risk is that the judge will simply authorise, without substantive review of the case, the requests for interceptions.

Conditions for the interception warrants for criminal investigation

Article 7 contains a list of conditions related to interception warrants for criminal investigations. While reference to “privacy”'s consideration is included in subparagraph 7(f), it does not specify the need to apply a test of necessity and proportionality to assess whether the envisaged interception measure does not exceed lawful interference with the rights to privacy or freedom of expression under international human rights standards.

Conditions for interception warrant for security reasons

Article 8 does not require any “privacy” or ‘freedom of expression’ impact assessment when issuing warrants of interception in the interest of state security (which remains undefined.) It only refers to “the importance of obtaining the information by interception is in the circumstances sufficient to justify the interception.” This is too vague a criterion to allow any proper assessment of the necessity and proportionality of the surveillance measure vis-a-vis its impact on individual's rights to privacy and freedom of expression.

Lack of regulation of use, storage and sharing of the intercepted communications

Nowhere in the draft Bill is there any provisions detailing the procedure to be followed for examining, using and storing the data obtained through the interception; the limits, safeguards and precautions to be taken when communicating the intercepted messages to other parties; and the circumstances in which intercepted communications may or must be erased or destroyed.

Unauthorised disclosure

Article 10 of the draft Bill imposes to a wide range of persons, including telecommunication service providers, an obligation to keep confidential the existence and contents of the interception warrants. Disclosure is considered an offence punishable also by imprisonment. Article 10(4) includes a limited grounds of defence in relation to a disclosure of a confidential matter.

Notably this list of defence does not include public interest. It is not known whether “public interest” is recognized under Ghanaian law as a lawful justification that can override the non-disclosure.

These provisions are likely to further limit the capacity of telecommunication service providers to publish statistics and other relevant information on interception of communications. Already Ghanaian law is limiting the publication of such information (see Vodaphone's report: https://www.vodafone.com/content/dam/sustainability/2014/pdf/vodafone_full_report_2014.pdf)

Further, the draft Bill contains no provision to require that those subjected to surveillance are notified that their communications have been intercepted, not even after the completion of the relevant investigation. This is a significant shortcoming which will negatively affect the right of individuals to seek redress for unlawful surveillance.

Obligations of telecommunications operators

Article 13(3) provides that when an interception warrant is served on a person who provides a telecommunication service or cyberspace telecommunication service, that person shall take the necessary action to enforce the warrant in the manner specified therein.

What steps can be imposed on telecommunication service providers is regulated in Article 14. The National Security Co-ordinator, without any need of judicial authorisation, can dictate such steps to ensure “the necessary practical interception capabilities”.

When it comes to configuring the telecommunication networks for “lawful interception”, Article 14(5) refers to the standards developed by the European Telecommunications Standards Institute, i.e. the technical protocols enacted across Europe for “lawful interception”. While these standards do not require direct, unmonitored access to the telecommunication network by the security agencies, the draft Bill imposes secrecy over the “existence of the equipment and packets or messages intercepted by means of the equipment” (Article 14(7)).

Decryption

Article 15(3) and (4) regulates the possibility of decrypting encrypted communications. According to Article 15(3)(b) decryption can only take place if the decryption key is provided. Additionally, Article 15(4) limits the obligations to decrypt by stating that service

providers cannot be required to have the “ability to decrypt a telecommunication message” or to impose an obligation to decrypt if “encryption is provided by means of a product that is supplied” by the telecommunication service.

The above suggests that the draft Bill does not empower the government to require service providers to establish “back doors” or otherwise require them to maintain a general capability to decrypt communications going through their networks. However, it remains unclear what powers can be exerted to obtain decryption keys. In light of the high risk of abuse, the regulation of decryption must be defined strictly the conditions and safeguards under which decryption order can be imposed. In the words of the UN Special Rapporteur on freedom of expression, “orders should be based on publicly accessible law, clearly limited in scope focused on a specific target, implemented under independent and impartial judicial authority, in particular to preserve the due process rights of targets, and only adopted when necessary and when less intrusive means of investigation are not available. Such measures may only be justified if used in targeting a specific user or users, subject to judicial oversight.” (UN Doc. A/HRC/29/32, paragraph 45.)

Supervision of the implementation

Article 18 provides that the Chief Justice “may” appoint a judge to supervise the implementation of the Act. The judge can initiate its own investigation, and require the relevant authorities to disclose “any information” in respect of the grant or the application for the authorisation. However such provision does not grant the judge the capacity to monitor and supervise the implementation of the interception warrants.

Every year, the judge shall submit a report on the application of the Act. The report is submitted to the National Security-Coordinator. There is no requirement that such report is published. Instead the National Security Co-ordinator shall submit an annual report to Parliament. Again there is no requirement of the report to be made public. Further, the report shall not contain information such as the names of the service providers who are providing assistance in the enforcement of the interception warrants.