Suggestions for privacy-relevant questions to be included in the List of Issues on the United Kingdom, Human Rights Committee, 112th Session

The right to privacy

The right to privacy is protected under Article 17 of the International Covenant on Civil and Political Rights. Article 17 provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on his honour or reputation.

Any surveillance activity, including the interception of communications, is an interference with the right to privacy[1] and can only be justified if it is in accordance with the law, has a legitimate objective and is conducted in a way that is necessary and proportionate. Surveillance activities must only be conducted when they are the only means of achieving a legitimate aim, or when there are multiple means, they are the least likely to infringe upon human rights.[2]

The United Kingdom is failing to uphold the right to privacy

Beginning in 1946, an alliance of five countries (the US, the UK, Australia, Canada and New Zealand) developed a series of bilateral agreements over more than a decade that became known as the UKUSA agreement, establishing the "Five Eyes" alliance for the purpose of sharing intelligence, but primarily signals intelligence.

In common with the legal frameworks of the other Five Eyes States, UK law distinguishes between the obligations owed to nationals or those within its territory, and non-nationals and those outside. The legislative framework pertaining to surveillance in the UK, the Regulation of Investigatory Powers Act 2000 (RIPA), distinguishes between "internal" and "external" interception, allowing for external communications to be intercepted without the need to establish any nexus with a particular person who is to be subject of the interception or a particular address that will be targeted. In doing so, the UK indirectly discriminates against non-British persons on grounds of nationality and national origin because of the distinction between internal and external communications, and the special protections granted to people in the UK under section 16 RIPA. A British person is more likely to be present in the British Islands and *vice versa*. An external communications warrant (issued under s8(4) of RIPA) is therefore likely to have a disparate adverse impact on non-British nationals.

As the High Commissioner for Human Rights recently noted in her report on the right to privacy in the digital age (A/HRC/27/37), international human rights law is explicit with regard to the

---

[1] Human Rights Committee General Comment 16, para. 8 ; see also Malone v United Kingdom (1985) 7 EHRR 14 [67].

[2] See, International Principles on the Application of Human Rights to Communications Surveillance, available at https://necessaryandproportionate.org

principle of non- discrimination, and the provisions of Article 26 ICCPR should be read together with article 17 to ensure that States do not take discriminatory measures in the context of the right to privacy. The Human Rights Committee has previously noted the importance of "measures to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are under direct surveillance."[3]

Further, there is no clear and accessible legal regime that indicates the circumstances in which intelligence sharing takes place within the Five Eyes alliance. It is clear that the UK's intelligence services can, at least in principle, obtain extensive access to communications and data that have been intercepted or obtained by the intelligence agencies of other Five Eyes states. However, there is no clear and explicit legal regime providing for the provision of and access to intercepted material by the UK. As the High Commissioner recently stated in her report, "any limitation to privacy rights reflected in article 17 must be provided for by law, and the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances." It is plain that the UK does not meet this threshold with respect to intelligence sharing.

We are also concerned by recent UK legislation on data retention. In July 2014 the UK parliament passed the Data Retention and Investigatory Powers Act, which continues[4] to allow for the mandatory blanket retention of communications data of the entire UK population for twelve months by providers of telecommunications services. In addition, the Act contains new powers, including allowing the government to require overseas companies to build interception capabilities into their products and infrastructure. The legislation was passed as an emergency measure, without sufficient parliamentary or public debate. Numerous human rights groups have expressed strong concerns about the law, as indiscriminate mandatory data retention is a disproportionate measure that violates the right to privacy.

Based on these observations, Privacy International proposes the following questions for the List of Issues:

Article 17

- What measures is the UK taking to ensure that the Five Eyes intelligence-sharing arrangement is governed and regulated by accessible, clear and precise laws?
- How does UK law on data retention comply with the state's obligations under the ICCPR, in particular article 17?

Article 26

- What measures is the UK taking to ensure that its communications interception regime complies with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are intercepted?

[3] CCPR /C/USA/CO/4, para. 22.
[4] This legislation followed a decision by the Court of Justice of the European Union that the European Union Data Retention Directive was invalid.